

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO. 074273/0163

Applicant: Satoshi OBANA

Title: ENCRYPTION AND DECRYPTION WITH ENDURANCE TO
CRYPTANALYSIS METHOD

Appl. No.: Unassigned

Filing Date: 04/20/2000

Examiner: Unassigned

Art Unit: Unassigned

Jc530 U.S. PTO
09/553415
04/20/00

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 11-114230 filed April 21, 1999.

Respectfully submitted,

April 20, 2000
Date

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

for / *Phillip J. Articola* Reg. No. 38,819
David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

OBANA
074273/0163

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 4月21日

出 願 番 号

Application Number:

平成11年特許願第114230号

出 願 人

Applicant (s):

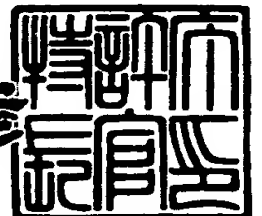
日本電気株式会社



2000年 2月18日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3007634

【書類名】 特許願

【整理番号】 33509445

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 尾花 賢

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088890

 【弁理士】

 【氏名又は名称】 河原 純一

【手数料の表示】

 【予納台帳番号】 009690

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9001717

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化装置、復号装置、および暗号化・復号装置

【特許請求の範囲】

【請求項 1】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、

平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、

前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化装置。

【請求項 2】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、

平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、

前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に

対する条件分岐決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化装置。

【請求項 3】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、

平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、

前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化装置。

【請求項 4】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段、平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段、および前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項 5】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続き

を選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段、平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段、および前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項 6】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段、平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段、および前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための暗号化処理プログラムを記録した記録媒体。

【請求項 7】 出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項 1，請求項 2，または請求項 3 記載の暗号化装置。

【請求項 8】 出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかである乱数生成装置の機能を有する暗号化処理プログラムを記録したことを特徴とする請求項 4，請求項 5，または請求項 6 記載の記録媒体。

【請求項 9】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、

暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、

前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段と

を備えたことを特徴とする復号装置。

【請求項 1 0】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、

暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、

前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする復号装置。

【請求項 1 1】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿

入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、

暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、

前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする復号装置。

【請求項 1 2】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段、暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段、および前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項 1 3】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段、暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させ

つつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段、および前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項 1 4】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段、暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段、および前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための復号処理プログラムを記録した記録媒体。

【請求項 1 5】 出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項 9、請求項 1 0、または請求項 1 1 記載の復号装置。

【請求項 1 6】 出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置の機能を有する復号処理プログラムを記録したことを特徴とする請求項 1 2、請求項 1 3、または請求項 1 4 記載の記録媒体。

【請求項 1 7】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、

処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、

前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化・復号装置。

【請求項 1 8】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、

処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、

前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化・復号装置。

【請求項 19】 乱数を出力する乱数生成装置と、

前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、

処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、

前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段と

を備えたことを特徴とする暗号化・復号装置。

【請求項 20】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段、処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段、ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適

用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項 2 1】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段、処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段、ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項 2 2】 コンピュータシステムを、乱数を出力する乱数生成装置、前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段、処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数

生成装置の出力に依存しない平文を出力する暗号化・復号演算手段，ならびに前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段として機能させるための暗号化・復号処理プログラムを記録した記録媒体。

【請求項 2 3】 暗号化処理の際に出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかであり、復号処理の際に出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置を備えたことを特徴とする請求項 1 7，請求項 1 8，または請求項 1 9 記載の暗号化・復号装置。

【請求項 2 4】 暗号化処理の際に出力するデータが暗号化を行う平文そのものおよび平文に依存したデータのいずれかであり、復号処理の際に出力するデータが復号を行う暗号文そのものおよび暗号文に依存したデータのいずれかである乱数生成装置の機能を有する暗号化・復号処理プログラムを記録したことを特徴とする請求項 2 0，請求項 2 1，または請求項 2 2 記載の記録媒体。

【請求項 2 5】 平文に加えて暗号化鍵を入力とする暗号化演算手段を備えることを特徴とする請求項 1，請求項 2，請求項 3，または請求項 7 記載の暗号化装置。

【請求項 2 6】 平文に加えて暗号化鍵を入力とする暗号化演算手段の機能を有する暗号化処理プログラムを記録したことを特徴とする請求項 4，請求項 5，請求項 6，または請求項 8 記載の記録媒体。

【請求項 2 7】 暗号文に加えて復号鍵を入力とする復号演算手段を備えることを特徴とする請求項 9，請求項 1 0，請求項 1 1，または請求項 1 5 記載の復号装置。

【請求項 2 8】 暗号文に加えて復号鍵を入力とする復号演算手段の機能を有する復号処理プログラムを記録したことを特徴とする請求項 1 2，請求項 1 3，請求項 1 4，または請求項 1 6 記載の記録媒体。

【請求項 2 9】 暗号化処理の際に処理データに加えて暗号化鍵を入力とし復号処理の際に処理データに加えて復号鍵を入力とする暗号化・復号演算手段を備

えることを特徴とする請求項 1 7, 請求項 1 8, 請求項 1 9, または請求項 2 3 記載の暗号化・復号装置。

【請求項 3 0】 暗号化処理の際に処理データに加えて暗号化鍵を入力とし復号処理の際に処理データに加えて復号鍵を入力とする暗号化・復号演算手段の機能を有する暗号化・復号処理プログラムを記録したことを特徴とする請求項 2 0, 請求項 2 1, 請求項 2 2, または請求項 2 4 記載の記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、暗号化鍵を用いて平文の暗号化を行い暗号文を生成する暗号化装置および復号鍵を用いて暗号文の復号を行い平文を生成する復号装置ならびに暗号化装置と復号装置との機能を併有する暗号化・復号装置に関する。なお、暗号化装置と復号装置とは、それぞれの入力異なるが構成や演算の内容は同様であるので、以下では主に暗号化装置で代表させて説明を行う。

【0 0 0 2】

【従来の技術】

従来の暗号化装置は、入力装置と記憶装置と暗号化処理装置と出力装置とから構成されており、次のように動作する。

【0 0 0 3】

すなわち、入力装置より暗号化処理装置に平文が入力され、平文を入力した暗号化処理装置は暗号化処理の中間段階で必要となる中間データを記憶装置に格納しつつ、常に予め定められた一定の処理順序に従って暗号化処理を行い、生成した暗号文を出力装置を通じて出力する。このとき、暗号化処理の開始時から特定の暗号化中間処理手続きが開始されるまでに要する時間は、おおよそ一定になる。

【0 0 0 4】

なお、暗号アルゴリズムの実装方法については、『「Applied Cryptography」(Bruce Schneier 著) John Wiley & Sons, Inc., 1996, ISBN 0-471-11709

-9, pp. 623-673』に詳しく述べられている。

【0005】

【発明が解決しようとする課題】

上述した従来の技術による暗号化装置には、電力解析（シンプル・パワー・アナリシス）や電力差分解析（ディファレンシャル・パワー・アナリシス）と呼ばれる暗号解析法が有効であるという問題が存在する。

【0006】

電力解析および電力差分解析は、現在のメモリやレジスタ等の半導体デバイスにおいて、特定の時刻に当該半導体デバイスの保持する値に変化があった場合に、当該時刻における消費電力が保持する値に変化がなかった場合と比較して大きくなるという特徴を利用して、暗号化装置が平文の暗号化を行っている複数の時点で暗号化装置が消費する電力を測定することにより、暗号化装置が保持している秘密鍵（暗号化鍵）等の秘密情報を特定する暗号解析法である。

【0007】

電力解析や電力差分解析が有効に機能する条件としては、第1に消費電力を測定している各時点で行われている暗号化処理手続きが特定できること、第2に各時刻で測定した消費電力の値が当該時刻において暗号化装置内で行われている暗号化処理の演算結果を顕著に反映していること、の2点が挙げられる。

【0008】

従来の暗号化装置（復号装置および暗号化・復号装置も同様）においては、上記の2点の条件が満たされてしまうために、先に述べたように、電力解析や電力差分解析が有効に機能し、暗号の解読が可能になりうるという問題点が存在した。

【0009】

本発明の目的は、上述の点に鑑み、暗号化処理（復号処理も同様）の処理過程において乱数依存の状態変化を起こすことにより、消費電力を測定している各時点で行われている暗号化処理手続きを特定することを困難にすることで、電力解析および電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置（同様な復号装置および暗号化・復号装置を含む）を提供することにあ

る。

【0010】

また、本発明の他の目的は、暗号化処理（復号処理も同様）の処理過程において乱数依存の状態変化を起こすことにより、各時刻で測定した消費電力の値と当該時刻に暗号化装置内で行われている暗号化処理との関連性を少なくすることで、電力解析および電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置（同様な復号装置および暗号化・復号装置を含む）を提供することにある。

【0011】

なお、本発明に対する従来技術に関する特許公報としては、特開平 9-230786 号公報および特開平 8-504067 号公報がある。

【0012】

上述の特開平 9-230786 号公報に記載された技術（データの暗号化方法及び装置）は、差分解読や線形解読を防止するための技術であり、暗号化の中間結果（本願発明における中間データ）を乱数には依存させずに変化させ、暗号化鍵を乱数に依存して変化させるものである。

【0013】

また、上述の特開平 8-504067 号公報に記載された技術（暗号化通信装置内の改善された機密性に関する方法および装置）は、電力遮断時等に、暗号化装置内の揮発性メモリに格納された鍵情報を能動的に消去し、電力供給再開時に同鍵情報をリロードするための技術である。

【0014】

これらの技術や当該両技術を組み合わせた技術では、最終的に出力される暗号文を乱数に依存しないようにすることは非常に困難である。これに対して、本発明の暗号化装置は、乱数生成装置によって出力される乱数に依存しない暗号文を出力するという性質を持っている（乱数に依存するのは中間データのみで、最終的な出力である暗号文は乱数に依存しない）。この点で、本発明は、上記の公報に記載された従来技術とは明確に異なっている。

【0015】

【課題を解決するための手段】

本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、平文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。

【0016】

また、本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、平文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【0017】

さらに、本発明の暗号化装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理中に意図的に挿入する実行

遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、平文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該平文に対する暗号化処理を実行し、当該平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力する暗号化演算手段と、前記暗号化演算手段による暗号化処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【0018】

本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、暗号文を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。

【0019】

また、本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、暗号文を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生

成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【0020】

さらに、本発明の復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、暗号文を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ当該暗号文に対する復号処理を実行し、当該暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する復号演算手段と、前記復号演算手段による復号処理の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【0021】

本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理実行中および復号処理実行中に必要な中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する中間データ制御手段と、処理データおよび処理内容を入力とし、前記中間データ制御手段による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段

階であると判断した場合に、前記中間データ制御手段に対する中間データ変更要求を発行する乱数依存性決定手段とを有する。

【0022】

また、本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理手続きおよび復号処理手続きの実行順序を決定することや複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択することを乱数に依存して行う乱数依存条件分岐決定操作を条件分岐決定要求の発生時点で行い、かつ暗号化・復号演算手段の出力が乱数に依存しないように当該乱数依存条件分岐決定操作を制御する条件分岐制御手段と、処理データおよび処理内容を入力とし、前記条件分岐制御手段による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存条件分岐決定操作を適用すべき処理段階であると判断した場合に、前記条件分岐制御手段に対する条件分岐決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【0023】

さらに、本発明の暗号化・復号装置は、乱数を出力する乱数生成装置と、前記乱数生成装置から出力される乱数を入力として、暗号化処理および復号処理中に意図的に挿入する実行遅延の遅延時間の決定を乱数に依存して行う乱数依存遅延挿入操作を遅延時間決定要求の発生時点で行う遅延制御手段と、処理データおよび処理内容を入力とし、前記遅延制御手段による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって前記乱数生成装置の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって前記乱数

生成装置の出力に依存しない平文を出力する暗号化・復号演算手段と、前記暗号化・復号演算手段による暗号化処理および復号処理の現在の処理段階が乱数依存遅延挿入操作を適用すべき処理段階であると判断した場合に、前記遅延制御手段に対する遅延時間決定要求を発行する乱数依存性決定手段とを有するように構成することも可能である。

【0024】

【発明の実施の形態】

次に、本発明について図面を参照して詳細に説明する。

【0025】

(1) 第1の実施の形態

図1は、本発明の第1の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0026】

本実施の形態に係る暗号化装置は、入力装置110と、暗号化処理装置120と、記憶装置130と、乱数生成装置140と、出力装置150とを含んで構成されている。

【0027】

これらの装置は、それぞれ、概略次のように動作する。

【0028】

入力装置110は、暗号化処理の対象となる平文を暗号化処理装置120に対して供給する。

【0029】

暗号化処理装置120は、乱数生成装置140から出力される乱数と入力装置110より入力される平文とを入力として、当該平文を暗号化処理装置120内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置150から出力する。

【0030】

ここで、暗号化処理装置120は、暗号化演算手段121と、乱数依存性決定手段122と、中間データ制御手段123とを備えている。

【0031】

暗号化演算手段 1 2 1 は、入力装置 1 1 0 を通して供給される平文を入力とし、暗号化演算手段 1 2 1 に格納されている暗号化鍵を用いて当該平文の暗号化を行う。暗号化演算手段 1 2 1 は、「中間データ制御手段 1 2 3 による中間データ（中間データ記憶部 1 3 1 に格納されているデータ）の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。なお、暗号化演算手段 1 2 1 は、暗号化処理実行中の複数の時点で、暗号化演算手段 1 2 1 による暗号化処理の現在の処理段階を乱数依存性決定手段 1 2 2 に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。

【0032】

乱数依存性決定手段 1 2 2 は、暗号化演算手段 1 2 1 が出力する暗号化演算手段 1 2 1 の現在の処理段階を入力として、当該処理段階に基づいて中間データ制御手段 1 2 3 に中間データ変更要求を出力すべきか否かを判断し、「中間データ変更要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には中間データ制御手段 1 2 3 に中間データ変更要求を出力する。

【0033】

中間データ制御手段 1 2 3 は、乱数依存性決定手段 1 2 2 より出力される中間データ変更要求を入力した場合に、乱数生成装置 1 4 0 に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して中間データ記憶部 1 3 1 に格納された中間データを変化させる操作（乱数依存中間データ変更操作）を行う。

【0034】

なお、中間データ制御手段 1 2 3 は、乱数依存中間データ変更操作を複数回適用することによって、乱数の効果を相殺するように構成されている。したがって、最終的に出力される暗号文は、乱数生成手段 1 4 0 から出力される乱数に依存しない。

【0035】

記憶装置 130 は、中間データ記憶部 131 を備えている。

【0036】

中間データ記憶部 131 は、暗号化処理装置 120 が行う暗号化処理中に保持する必要のある中間データを格納する。なお、上記に示す通り、乱数依存性決定手段 122 から中間データ制御手段 123 に中間データ変更要求があった場合には、中間データ記憶部 131 に格納されている中間データは中間データ制御手段 123 によって操作される。

【0037】

乱数生成装置 140 は、暗号化処理装置 120 より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置 120 に乱数を出力する。

【0038】

図 2 は、本実施の形態に係る暗号化装置の処理を示す流れ図である。この処理は、平文入力ステップ A1 と、中間データ変更要求有無判定ステップ A2 と、乱数出力ステップ A3 と、乱数依存中間データ変更操作ステップ A4 と、暗号化処理一段階実行ステップ A5 と、暗号化処理終了判定ステップ A6 と、暗号文出力ステップ A7 とからなる。

【0039】

次に、図 1 および図 2 を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。

【0040】

まず、暗号化を行いたい平文が、入力装置 110 から暗号化処理装置 120 内の暗号化演算手段 121 に入力される（図 2 のステップ A1）。

【0041】

暗号化演算手段 121 は、暗号化演算手段 121 による暗号化処理の現在の処理段階を乱数依存性決定手段 122 に出力する。

【0042】

乱数依存性決定手段 122 は、暗号化演算手段 121 より受け取った暗号化演算手段 121 の処理段階に関する情報を基に、現在の処理段階が中間データ記憶

部 1 3 1 に格納された中間データを乱数に依存して変更する処理段階であるか否かの判断を行い、「乱数に依存して中間データを変更する処理段階である」と判断した場合には中間データ制御手段 1 2 3 に中間データ変更要求を出力する。

【0 0 4 3】

中間データ制御手段 1 2 3 は、乱数依存性決定手段 1 2 2 からの中間データ変更要求があるか否かを判定する（ステップ A 2）。

【0 0 4 4】

中間データ制御手段 1 2 3 は、ステップ A 2 で「中間データ変更要求がある」と判定した場合には、当該中間データ変更要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置 1 4 0 に送り、当該乱数要求信号に基づいて乱数生成装置 1 4 0 から出力された乱数を得る（ステップ A 3）。

【0 0 4 5】

乱数を受け取った中間データ制御手段 1 2 3 は、記憶装置 1 3 0 内の中間データ記憶部 1 3 1 に格納されている中間データ（暗号化処理手段 1 2 1 が暗号化処理の中間段階において必要とするデータ）を受け取った乱数に依存して変更する乱数依存中間データ変更操作を行う（ステップ A 4）。

【0 0 4 6】

暗号化演算手段 1 2 1 は、ステップ A 4 の乱数依存中間データ変更操作が終了した後に、またはステップ A 2 で「中間データ変更要求がない」と判定した場合に、暗号化処理を一段階実行する（ステップ A 5）。

【0 0 4 7】

暗号化演算手段 1 2 1 は、暗号化処理を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップ A 6）。

【0 0 4 8】

暗号化演算手段 1 2 1 は、ステップ A 6 で「暗号化処理を一段階実行したことで暗号化処理が終了した」と判定した場合には、出力装置 1 5 0 に暗号文を出力し（ステップ A 7）、全体の処理を終了させる。

【0 0 4 9】

一方、暗号化演算手段 1 2 1 は、ステップ A 6 で「暗号化処理が終了していな

い」と判定した場合（暗号化処理がまだ残されている場合）には、ステップ A 2 に制御を戻して暗号化処理を継続させる。

【0050】

次に、本実施の形態における効果について説明する。

【0051】

本実施の形態では、暗号化処理の中間段階で必要なデータ（中間データ）が乱数に依存して変化しているために、中間データ間の演算を行っている時点の電力を測定することによって格納されている中間データの情報を引き出そうとしても、中間データの値が乱数による影響を受けているために消費電力の変化が生じているのか、実際の暗号化処理に必要なデータの影響によって消費電力の変化が生じているのかを判断することが困難になる。したがって、暗号化装置を電力解析や電力差分析による暗号解析に対して耐性があるようにすることができる。

【0052】

（2） 第2の実施の形態

図3は、本発明の第2の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0053】

図3を参照すると、本実施の形態に係る暗号化装置は、入力装置310と、暗号化処理装置320と、記憶装置330と、乱数生成装置340と、出力装置350とを含んで構成されている。

【0054】

これらの装置は、それぞれ、概略次のように動作する。

【0055】

入力装置310は、暗号化処理の対象となる平文を暗号化処理装置320に対して供給する。

【0056】

暗号化処理装置320は、乱数生成装置340から出力される乱数と入力装置310より入力される平文とを入力として、当該平文を暗号化処理装置320の内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置350から出力

する。

【0057】

ここで、暗号化処理装置 3 2 0 は、暗号化演算手段 3 2 1 と、乱数依存性決定手段 3 2 2 と、条件分岐制御手段 3 2 3 とを備えている。

【0058】

暗号化演算手段 3 2 1 は、入力装置 3 1 0 を通して供給される平文を入力とし、暗号化演算手段 3 2 1 に格納されている暗号化鍵を用いて当該平文の暗号化を行う。暗号化演算手段 3 2 1 は、「条件分岐制御手段 3 2 3 による命令実行順序（暗号化処理手続きの実行順序）の決定および実行命令の選択（複数の処理手続きの選択肢の中から実際に実行される処理手続きを選択すること）の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。なお、暗号化演算手段 3 2 1 は、暗号化処理実行中の複数の時点で、暗号化演算手段 3 2 1 による暗号化処理の現在の処理段階を乱数依存性決定手段 3 2 2 に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。

【0059】

乱数依存性決定手段 3 2 2 は、暗号化演算手段 3 2 1 が出力する暗号化演算手段 3 2 1 の現在の処理段階を入力として、当該処理段階に基づいて条件分岐制御手段 3 2 3 に条件分岐決定要求を出力すべきか否かを判断し、「条件分岐決定要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には条件分岐制御手段 3 2 4 に条件分岐決定要求を出力する。

【0060】

条件分岐制御手段 3 2 3 は、乱数依存性決定手段 3 2 2 より出力される条件分岐決定要求を入力した場合に、乱数生成装置 3 4 0 に乱数要求信号を送ることにによって乱数を取得し、取得した乱数に依存して「実行順序を交換しても暗号化演算手段 3 2 1 の出力が変化しないような複数の暗号化処理手続きの実行順序の決定」および「どの処理手続きを実行しても暗号化演算手段 3 2 1 の出力が変化し

ないような複数の処理手続きの選択肢の中からの実行処理手続き（実際に実行する暗号化処理手続き）の選択」を行う操作（乱数依存条件分岐決定操作）を行う。

【0061】

なお、条件分岐制御手段 3 2 3 は、前述のように暗号化演算手段 3 2 1 の出力が乱数に依存しないように乱数依存条件分岐決定操作を制御するように構成されている。したがって、最終的に出力される暗号文は、乱数生成手段 3 4 0 から出力される乱数に依存しない。

【0062】

記憶装置 3 3 0 は、中間データ記憶部 3 3 1 を備えている。

【0063】

中間データ記憶部 3 3 1 は、暗号化処理装置 3 2 0 が行う暗号化処理中に保持する必要のある中間データを格納する。

【0064】

乱数生成装置 3 4 0 は、暗号化処理装置 3 2 0 より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置 3 2 0 に乱数を出力する。

【0065】

図 4 は、本実施の形態に係る暗号化装置の処理を示す流れ図である。この処理は、平文入力ステップ B 1 と、条件分岐決定要求有無判定ステップ B 2 と、乱数出力ステップ B 3 と、乱数依存条件分岐決定操作ステップ B 4 と、暗号化処理一段階実行ステップ B 5 と、暗号化処理終了判定ステップ B 6 と、暗号文出力ステップ B 7 とからなる。

【0066】

次に、図 3 および図 4 を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。

【0067】

まず、暗号化を行いたい平文が、入力装置 3 1 0 から暗号化処理装置 3 2 0 内の暗号化演算手段 3 2 1 に入力される（図 4 のステップ B 1）。

【0068】

暗号化演算手段 3 2 1 は、暗号化演算手段 3 2 1 における暗号化処理の現在の処理段階を乱数依存性決定手段 3 2 2 に出力する。

【0 0 6 9】

乱数依存性決定手段 3 2 2 は、暗号化演算手段 3 2 1 より受け取った暗号化演算手段 3 2 1 の処理段階に関する情報を基に、現在の処理段階が乱数に依存した条件分岐の決定を行う処理段階であるか否かの判断を行い、「乱数に依存した条件分岐の決定を行う処理段階である」と判断した場合には条件分岐制御手段 3 2 3 に条件分岐決定要求を出力する。

【0 0 7 0】

条件分岐制御手段 3 2 3 は、乱数依存性決定手段 3 2 2 からの条件分岐決定要求があるか否かを判定する（ステップ B 2）。

【0 0 7 1】

条件分岐制御手段 3 2 3 は、ステップ B 2 で「条件分岐決定要求がある」と判定した場合には、当該条件分岐決定要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置 3 4 0 に送り、当該乱数要求信号に基づいて乱数生成装置 3 4 0 から出力された乱数を得る（ステップ B 3）。

【0 0 7 2】

乱数を受け取った条件分岐制御手段 3 2 3 は、受け取った乱数に依存して出力結果が同一となる複数の処理手続きの中から実際に行う処理手続きを選択等する乱数依存条件分岐決定操作を行う（ステップ B 4）。

【0 0 7 3】

暗号化演算手段 3 2 1 は、ステップ B 4 の乱数依存条件分岐決定操作が終了した後に、またはステップ B 2 で「条件分岐決定要求がない」と判定した場合には、暗号化処理を一段階実行する（ステップ B 5）。

【0 0 7 4】

暗号化演算手段 3 2 1 は、暗号化を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップ B 6）。

【0 0 7 5】

暗号化演算手段 3 2 1 は、ステップ B 6 で「暗号化を一段階実行したことで暗

号化処理が終了した」と判定した場合には、出力装置 3 5 0 に暗号文を出力し（ステップ B 7）、全体の処理を終了させる。

【0 0 7 6】

一方、暗号化演算手段 3 2 1 は、ステップ B 6 で「暗号化処理が終了していない」と判定した場合（暗号化処理がまだ残されている場合）には、ステップ B 2 に制御を戻して暗号化処理を継続させる。

【0 0 7 7】

次に、本実施の形態における効果について説明する。

【0 0 7 8】

本実施の形態では、乱数によって実行される暗号化処理の順序や種類が変化するために、特定の時刻に着目しても当該時刻において暗号化処理装置 3 2 0 の内部で行われている処理が乱数によって異なっており、消費電力の変化を観測しても当該消費電力の変化がどの暗号化処理に対応しているのかを判断することが困難になる。したがって、暗号化装置を電力解析や電力差分解析による暗号解析に対して耐性があるようにすることができる。

【0 0 7 9】

（3） 第 3 の実施の形態

図 5 は、本発明の第 3 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0 0 8 0】

図 5 を参照すると、本発明の実施の形態に係る暗号化装置は、入力装置 5 1 0 と、暗号化処理装置 5 2 0 と、記憶装置 5 3 0 と、乱数生成装置 5 4 0 と、出力装置 5 5 0 とを含んで構成されている。

【0 0 8 1】

これらの装置は、それぞれ、概略次のように動作する。

【0 0 8 2】

入力装置 5 1 0 は、暗号化処理の対象となる平文を暗号化処理装置 5 2 0 に対して供給する。

【0 0 8 3】

暗号化処理装置 5 2 0 は、乱数生成装置 5 4 0 から出力される乱数と入力装置 5 1 0 より入力される平文とを入力として、当該平文を暗号化処理装置 5 2 0 の内部に格納された鍵（暗号化鍵）で暗号化した暗号文を出力装置 5 5 0 から出力する。

【0 0 8 4】

ここで、暗号化処理装置 5 2 0 は、暗号化演算手段 5 2 1 と、乱数依存性決定手段 5 2 2 と、遅延制御手段 5 2 3 とを備えている。

【0 0 8 5】

暗号化演算手段 5 2 1 は、入力装置 5 1 0 を通して供給される平文を入力とし、暗号化演算手段 5 2 1 に格納されている暗号化鍵を用いて当該平文の暗号化を行う。暗号化演算手段 5 2 1 は、「遅延制御手段 5 2 3 による実行遅延時間の決定の乱数に依存した変更」を受けて状態を変化させつつ暗号化処理（複数の処理段階によって形成される暗号化処理）を実行し、最終的に当該平文を暗号化した暗号文を出力する。なお、暗号化演算手段 5 2 1 は、暗号化処理実行中の複数の時点で、暗号化演算手段 5 2 1 による暗号化処理の現在の処理段階を乱数依存性決定手段 5 2 2 に送る（これにより、適切な処理段階で乱数に依存した状態の変化を生じさせることができる）。

【0 0 8 6】

乱数依存性決定手段 5 2 2 は、暗号化演算手段 5 2 1 が出力する暗号化演算手段 5 2 1 の現在の処理段階を入力として、当該処理段階に基づいて遅延制御手段 5 2 3 に遅延時間決定要求を出力すべきか否かを判断し、「遅延時間決定要求の出力」を決定した場合（現在の処理段階が乱数に依存した操作を適用すべき処理段階であると判断した場合）には遅延制御手段 5 2 3 に遅延時間決定要求を出力する。

【0 0 8 7】

遅延制御手段 5 2 3 は、乱数依存性決定手段 5 2 2 より出力される遅延時間決定要求を入力した場合に、乱数生成装置 5 4 0 に乱数要求信号を送ることによって乱数を取得し、取得した乱数に依存して暗号化処理中に意図的に発生させる実行遅延の遅延時間を決定して当該遅延を挿入する操作（乱数依存遅延挿入操作）

を行う。

【0088】

なお、遅延制御手段523は、暗号化演算手段521の処理に取得した乱数に応じた遅延を挿入する操作を行うように構成されており、遅延の挿入は暗号化に必要なデータにまったく乱数の影響をおよぼさない。したがって、最終的に出力される暗号文は、乱数生成手段540から出力される乱数に依存しない。

【0089】

記憶装置530は、中間データ記憶部531を備えている。

【0090】

中間データ記憶部531は、暗号化処理装置520が行う暗号化処理中に保持する必要のある中間データを格納する。

【0091】

乱数生成装置540は、暗号化処理装置520より乱数要求信号を受け取り、当該乱数要求信号に基づいて暗号化処理装置520に乱数を出力する。

【0092】

図6は、本実施の形態に係る暗号化装置の処理を示す流れ図である。この処理は、平文入力ステップC1と、遅延時間決定要求有無判定ステップC2と、乱数出力ステップC3と、乱数依存遅延挿入操作ステップC4と、暗号化処理一段階実行ステップC5と、暗号化処理終了判定ステップC6と、暗号文出力ステップC7とからなる。。

【0093】

次に、図5および図6を参照して、本実施の形態に係る暗号化装置の全体の動作について詳細に説明する。

【0094】

まず、暗号化を行いたい平文が、入力装置510から暗号化処理装置520内の暗号化演算手段521に入力される（図6のステップC1）。

【0095】

暗号化演算手段521は、暗号化演算手段521における暗号化処理の現在の処理段階を乱数依存性決定手段522に出力する。

【0096】

乱数依存性決定手段522は、暗号化演算手段521より受け取った暗号化演算手段521の処理段階に関する情報を基に、現在の処理段階が乱数に依存した遅延を挿入する処理段階（当該遅延の遅延時間を決定する処理段階）であるか否かの判断を行い、「乱数に依存した遅延を挿入する処理段階である」と判断した場合には遅延制御手段523に遅延時間決定要求を出力する。

【0097】

遅延制御手段523は、乱数依存性決定手段522からの遅延時間決定要求があるか否かを判定する（ステップC2）。

【0098】

遅延制御手段523は、ステップC2で「遅延時間決定要求がある」と判定した場合には、当該遅延時間決定要求を受け取り、乱数要求（乱数要求信号）を乱数生成装置540に送り、当該乱数要求信号に基づいて乱数生成装置540から出力された乱数を得る（ステップC3）。

【0099】

乱数を受け取った遅延制御手段523は、受け取った乱数に依存して遅延時間を決定し、決定した遅延時間の実行遅延を暗号化処理中に意図的に挿入する（ステップC4）。

【0100】

暗号化演算手段521は、ステップC4の乱数依存遅延挿入操作が終了した後に、またはステップB2で「乱数依存遅延時間決定要求がない」と判定した場合には、暗号化処理を一段階実行する（ステップC5）。

【0101】

暗号化演算手段521は、暗号化を一段階実行したことで暗号化処理が終了したか否かを判定する（ステップC6）。

【0102】

暗号化演算手段521は、ステップC6で「暗号化を一段階実行したことで暗号化処理が終了した」と判定した場合には、出力装置550に暗号文を出力し（ステップC7）、全体の処理を終了させる。

【0103】

一方、暗号化演算手段 5 2 1 は、ステップ C 6 で「暗号化処理が終了していない」と判定した場合（暗号化処理がまだ残されている場合）には、ステップ C 2 に制御を戻して暗号化処理を継続させる。

【0104】

次に、本実施の形態における効果について説明する。

【0105】

本実施の形態では、乱数に依存した遅延時間の実行遅延が適宜挿入されるために、暗号解析に有用となる処理が行われている時刻が絶えず変化し、どの時刻の消費電力の変化に着目すれば効率的に暗号解析に必要な情報を得ることができるのかを特定することが困難になる。したがって、暗号化装置を電力解析や電力差分析による暗号解析に対して耐性があるようにすることができる。

【0106】

なお、上述の第 1，第 2，および第 3 の実施の形態に係る暗号化装置においては、暗号化鍵が予め暗号化演算手段（図 1 中の暗号化演算手段 1 2 1，図 3 中の暗号化演算手段 3 2 1，および図 5 中の暗号化演算手段 5 2 1）に格納されていた。

【0107】

しかし、入力装置（図 1 中の入力装置 1 1 0，図 3 中の入力装置 3 1 0，および図 5 中の入力装置 5 1 0）から暗号化演算手段に暗号化鍵を入力するように、上記の暗号化装置を構成することも可能である。この場合には、暗号化鍵を入力された暗号化演算手段は、その後に入力される 1 つまたは複数の平文の暗号化を当該暗号化鍵を用いて行い、暗号文を出力する。

【0108】

上記のような構成を採用すると、暗号化鍵を外部から入力するようにできるため、暗号化演算手段自体を変更せずに暗号化鍵の更新を容易に行うことができるようになる。

【0109】

また、上述の第 1，第 2，および第 3 の実施の形態に係る暗号化装置において

は、乱数生成装置（図 1 中の乱数生成装置 1 4 0，図 3 中の乱数生成装置 3 4 0，および図 5 中の乱数生成装置 5 4 0）から出力される乱数を、入力装置から暗号化处理装置（図 1 中の暗号化处理装置 1 2 0，図 3 中の暗号化处理装置 3 2 0，および図 5 中の暗号化处理装置 5 2 0）に入力されるデータ（平文）そのものまたは当該データに依存したデータとすることも可能である。

【0 1 1 0】

このように平文を「乱数」として使用することが可能かつ有効になるのは、現在提案されている電力解析および電力差分解析では暗号文と消費電力とのみから暗号解析が行われており、平文のデータは暗号解析に使用されていないため、平文を乱数として利用することができるからである。なお、乱数として「平文に依存したデータ」を用いるということは、例えば入力装置に入力される平文を暗号化鍵とは別の「乱数出力用鍵」で暗号化し、その暗号化の出力を乱数として利用するという暗号化装置も、本発明に含まれることになる。

【0 1 1 1】

（4） 第 4 の実施の形態

図 7 は、本発明の第 4 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0 1 1 2】

図 7 を参照すると、本発明の第 4 の実施の形態に係る暗号化装置は、図 1 に示した第 1 の実施の形態に係る暗号化装置に対して、暗号化处理プログラムを記録した記録媒体 7 0 0 を備える点が異なっている。この記録媒体 7 0 0 は、磁気ディスク、半導体メモリ、CD-ROM (Compact Disk-Read Only Memory)，その他の記録媒体であってよい。

【0 1 1 3】

暗号化处理プログラムは、記録媒体 7 0 0 からコンピュータシステム（入力装置 1 1 0，暗号化处理装置 1 2 0，記憶装置 1 3 0，乱数生成装置 1 4 0，および出力装置 1 5 0 を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置 1 1 0，暗号化处理装置 1 2 0（暗号化演算手段 1 2 1，乱数依存性決定手段 1 2 2，および中間データ制御手段 1 2 3），記憶

装置 1 3 0 (中間データ記憶部 1 3 1), 乱数生成装置 1 4 0, および出力装置 1 5 0 として制御する。暗号化処理プログラムの制御による入力装置 1 1 0, 暗号化処理装置 1 2 0, 記憶装置 1 3 0, 乱数生成装置 1 4 0, および出力装置 1 5 0 の動作は、第 1 の実施の形態における入力装置 1 1 0, 暗号化処理装置 1 2 0, 記憶装置 1 3 0, 乱数生成装置 1 4 0, および出力装置 1 5 0 の動作と全く同様になるので、その詳しい説明を割愛する。

【0 1 1 4】

(5) 第 5 の実施の形態

図 8 は、本発明の第 5 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0 1 1 5】

図 8 を参照すると、本発明の第 5 の実施の形態に係る暗号化装置は、図 3 に示した第 2 の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体 8 0 0 を備える点が異なっている。この記録媒体 8 0 0 は、磁気ディスク、半導体メモリ、CD-ROM, その他の記録媒体であってよい。

【0 1 1 6】

暗号化処理プログラムは、記録媒体 8 0 0 からコンピュータシステム (入力装置 3 1 0, 暗号化処理装置 3 2 0, 記憶装置 3 3 0, 乱数生成装置 3 4 0, および出力装置 3 5 0 を備えるコンピュータシステム) に読み込まれ、当該コンピュータシステムの動作を入力装置 3 1 0, 暗号化処理装置 3 2 0 (暗号化演算手段 3 2 1, 乱数依存性決定手段 3 2 2, および条件分岐制御手段 3 2 3), 記憶装置 3 3 0 (中間データ記憶部 3 3 1), 乱数生成装置 3 4 0, および出力装置 3 5 0 として制御する。暗号化処理プログラムの制御による入力装置 3 1 0, 暗号化処理装置 3 2 0, 記憶装置 3 3 0, 乱数生成装置 3 4 0, および出力装置 3 5 0 の動作は、第 2 の実施の形態における入力装置 3 1 0, 暗号化処理装置 3 2 0, 記憶装置 3 3 0, 乱数生成装置 3 4 0, および出力装置 3 5 0 の動作と全く同様になるので、その詳しい説明を割愛する。

【0 1 1 7】

(6) 第 6 の実施の形態

図 9 は、本発明の第 6 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【0118】

図 9 を参照すると、本発明の第 6 の実施の形態に係る暗号化装置は、図 5 に示した第 3 の実施の形態に係る暗号化装置に対して、暗号化処理プログラムを記録した記録媒体 900 を備える点が異なっている。この記録媒体 900 は、磁気ディスク、半導体メモリ、CD-ROM、その他の記録媒体であってよい。

【0119】

暗号化処理プログラムは、記録媒体 900 からコンピュータシステム（入力装置 510、暗号化処理装置 520、記憶装置 530、乱数生成装置 540、および出力装置 550 を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置 510、暗号化処理装置 520（暗号化演算手段 521、乱数依存性決定手段 522、および遅延制御手段 523）、記憶装置 530（中間データ記憶部 531）、乱数生成装置 540、および出力装置 550 として制御する。暗号化処理プログラムの制御による入力装置 510、暗号化処理装置 520、記憶装置 530、乱数生成装置 540、および出力装置 550 の動作は、第 3 の実施の形態における入力装置 510、暗号化処理装置 520、記憶装置 530、乱数生成装置 540、および出力装置 550 の動作と全く同様になるので、その詳しい説明を割愛する。

【0120】

（7） 第 7 の実施の形態

図 10 は、本発明の第 7 の実施の形態に係る復号装置の構成を示すブロック図である。

【0121】

図 10 を参照すると、本実施の形態に係る復号装置は、入力装置 1010 と、復号演算手段 1021、乱数依存性決定手段 1022、および中間データ制御手段 1023 を備える復号処理装置 1020 と、中間データ記憶部 1031 を備える記憶装置 1030 と、乱数生成装置 1040 と、出力装置 1050 とを含んで構成されている。

【0 1 2 2】

本実施の形態に係る復号装置は、第 1 の実施の形態に係る暗号化装置と同様に、入力装置、復号処理装置（暗号化処理装置に該当する）、記憶装置、乱数生成装置、および出力装置を備えている。ここで、第 1 の実施の形態では、入力装置 1 1 0 からは平文が入力され、暗号化処理装置 1 2 0 が暗号化鍵を用いて平文の暗号化を行い、出力装置 1 5 0 から暗号文が出力されていた。これに対し、本実施の形態では、入力装置 1 0 1 0 からは暗号文が入力され、復号処理装置 1 0 2 0 が復号鍵を用いて暗号文の復号を行い、出力装置 1 0 5 0 から平文が出力される。上記の点で、本実施の形態に係る復号装置は第 1 の実施の形態に係る暗号化装置と異なっている（それ以外の構成や動作は同様である）。

【0 1 2 3】

(8) 第 8 の実施の形態

図 1 1 は、本発明の第 8 の実施の形態に係る復号装置の構成を示すブロック図である。

【0 1 2 4】

図 1 1 を参照すると、本実施の形態に係る復号装置は、入力装置 1 1 1 0 と、復号演算手段 1 1 2 1、乱数依存性決定手段 1 1 2 2、および条件分岐制御手段 1 1 2 3 を備える復号処理装置 1 1 2 0 と、中間データ記憶部 1 1 3 1 を備える記憶装置 1 1 3 0 と、乱数生成装置 1 1 4 0 と、出力装置 1 1 5 0 とを含んで構成されている。

【0 1 2 5】

本実施の形態に係る復号装置は、第 2 の実施の形態に係る暗号化装置と同様に、入力装置、復号処理装置（暗号化処理装置に該当する）、記憶装置、乱数生成装置、および出力装置を備えている。ここで、第 2 の実施の形態では、入力装置 3 1 0 からは平文が入力され、暗号化処理装置 3 2 0 が暗号化鍵を用いて平文の暗号化を行い、出力装置 3 5 0 から暗号文が出力されていた。これに対し、本実施の形態では、入力装置 1 1 1 0 からは暗号文が入力され、復号処理装置 1 1 2 0 が復号鍵を用いて暗号文の復号を行い、出力装置 1 1 5 0 から平文が出力される。上記の点で、本実施の形態に係る復号装置は第 2 の実施の形態に係る暗号化

装置と異なっている（それ以外の構成や動作は同様である）。

【0 1 2 6】

（9） 第9の実施の形態

図12は、本発明の第9の実施の形態に係る復号装置の構成を示すブロック図である。

【0 1 2 7】

図12を参照すると、本実施の形態に係る復号装置は、入力装置1210と、復号演算手段1221、乱数依存性決定手段1222、および遅延制御手段1223を備える復号処理装置1220と、中間データ記憶部1231を備える記憶装置1230と、乱数生成装置1240と、出力装置1250とを含んで構成されている。

【0 1 2 8】

本実施の形態に係る復号装置は、第3の実施の形態に係る暗号化装置と同様に、入力装置、復号処理装置（暗号化処理装置に該当する）、記憶装置、乱数生成装置、および出力装置を備えている。ここで、第3の実施の形態では、入力装置510からは平文が入力され、暗号化処理装置520が暗号化鍵を用いて平文の暗号化を行い、出力装置550から暗号文が出力されていた。これに対し、本実施の形態では、入力装置1210からは暗号文が入力され、復号処理装置1220が復号鍵を用いて暗号文の復号を行い、出力装置1250から平文が出力される。上記の点で、本実施の形態に係る復号装置は第3の実施の形態に係る暗号化装置と異なっている（それ以外の構成や動作は同様である）。

【0 1 2 9】

なお、上述の第7、第8、および第9の実施の形態に係る復号装置においては、入力装置（図10中の入力装置1010、図11中の入力装置1110、および図12中の入力装置1210）から復号演算手段（図10中の復号演算手段1021、図11中の復号演算手段1121、および図12中の復号演算手段1221）に復号鍵を入力するように構成することも可能である。

【0 1 3 0】

また、上述の第7、第8、および第9の実施の形態に係る復号装置においては

、乱数生成装置（図 1 0 中の乱数生成装置 1 0 4 0，図 1 1 中の乱数生成装置 1 1 4 0，および図 1 2 中の乱数生成装置 1 2 4 0）から出力される乱数を、入力装置から復号処理装置（図 1 0 中の復号処理装置 1 0 2 0，図 1 1 中の復号処理装置 1 1 2 0，および図 1 2 中の復号処理装置 1 2 2 0）に入力されるデータ（暗号文）そのものまたは当該データに依存したデータとすることも可能である。

【0 1 3 1】

（1 0） 第 1 0 の実施の形態

図 1 3 は、本発明の第 1 0 の実施の形態に係る復号装置の構成を示すブロック図である。

【0 1 3 2】

図 1 3 を参照すると、本発明の第 1 0 の実施の形態に係る復号装置は、図 1 0 に示した第 7 の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体 1 3 0 0 を備える点が異なっている。この記録媒体 1 3 0 0 は、磁気ディスク、半導体メモリ、CD-ROM、その他の記録媒体であってよい。

【0 1 3 3】

復号処理プログラムは、記録媒体 1 3 0 0 からコンピュータシステム（入力装置 1 0 1 0，復号処理装置 1 0 2 0，記憶装置 1 0 3 0，乱数生成装置 1 0 4 0，および出力装置 1 0 5 0 を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置 1 0 1 0，復号処理装置 1 0 2 0（復号演算手段 1 0 2 1，乱数依存性決定手段 1 0 2 2，および中間データ制御手段 1 0 2 3），記憶装置 1 0 3 0（中間データ記憶部 1 0 3 1），乱数生成装置 1 0 4 0，および出力装置 1 0 5 0 として制御する。復号処理プログラムの制御による入力装置 1 0 1 0，復号処理装置 1 0 2 0，記憶装置 1 0 3 0，乱数生成装置 1 0 4 0，および出力装置 1 0 5 0 の動作は、第 7 の実施の形態における入力装置 1 0 1 0，復号処理装置 1 0 2 0，記憶装置 1 0 3 0，乱数生成装置 1 0 4 0，および出力装置 1 0 5 0 の動作と全く同様になるので、その詳しい説明を割愛する。

【0 1 3 4】

(11) 第11の実施の形態

図14は、本発明の第11の実施の形態に係る復号装置の構成を示すブロック図である。

【0135】

図14を参照すると、本発明の第11の実施の形態に係る復号装置は、図11に示した第8の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体1400を備える点が異なっている。この記録媒体1400は、磁気ディスク、半導体メモリ、CD-ROM、その他の記録媒体であってよい。

【0136】

復号処理プログラムは、記録媒体1400からコンピュータシステム（入力装置1110、復号処理装置1120、記憶装置1130、乱数生成装置1140、および出力装置1150を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置1110、復号処理装置1120（復号演算手段1121、乱数依存性決定手段1122、および条件分岐制御手段1123）、記憶装置1130（中間データ記憶部1131）、乱数生成装置1140、および出力装置1150として制御する。復号処理プログラムの制御による入力装置1110、復号処理装置1120、記憶装置1130、乱数生成装置1140、および出力装置1150の動作は、第8の実施の形態における入力装置1110、復号処理装置1120、記憶装置1130、乱数生成装置1140、および出力装置1150の動作と全く同様になるので、その詳しい説明を割愛する。

【0137】

(12) 第12の実施の形態

図15は、本発明の第12の実施の形態に係る復号装置の構成を示すブロック図である。

【0138】

図15を参照すると、本発明の第12の実施の形態に係る復号装置は、図12に示した第9の実施の形態に係る復号装置に対して、復号処理プログラムを記録した記録媒体1500を備える点が異なっている。この記録媒体1500は、磁

気ディスク、半導体メモリ、CD-ROM、その他の記録媒体であってよい。

【0139】

復号処理プログラムは、記録媒体 1 5 0 0 からコンピュータシステム（入力装置 1 2 1 0、復号処理装置 1 2 2 0、記憶装置 1 2 3 0、乱数生成装置 1 2 4 0、および出力装置 1 2 5 0 を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置 1 2 1 0、復号処理装置 1 2 2 0（復号演算手段 1 2 2 1、乱数依存性決定手段 1 2 2 2、および遅延制御手段 1 2 2 3）、記憶装置 1 2 3 0（中間データ記憶部 1 2 3 1）、乱数生成装置 1 2 4 0、および出力装置 1 2 5 0 として制御する。復号処理プログラムの制御による入力装置 1 2 1 0、復号処理装置 1 2 2 0、記憶装置 1 2 3 0、乱数生成装置 1 2 4 0、および出力装置 1 2 5 0 の動作は、第 9 の実施の形態における入力装置 1 2 1 0、復号処理装置 1 2 2 0、記憶装置 1 2 3 0、乱数生成装置 1 2 4 0、および出力装置 1 2 5 0 の動作と全く同様になるので、その詳しい説明を割愛する。

【0140】

(13) 第 13 の実施の形態

図 1 6 は、本発明の第 13 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【0141】

図 1 6 を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置 1 6 1 0 と、暗号化・復号演算手段 1 6 2 1、乱数依存性決定手段 1 6 2 2、および中間データ制御手段 1 6 2 3 を備える暗号化・復号処理装置 1 6 2 0 と、中間データ記憶部 1 6 3 1 を備える記憶装置 1 6 3 0 と、乱数生成装置 1 6 4 0 と、出力装置 1 6 5 0 とを含んで構成されている。

【0142】

本実施の形態に係る暗号化・復号装置は、第 1 の実施の形態に係る暗号化装置の機能と第 7 の実施の形態に係る復号装置の機能とを併有している。ここで、入力装置 1 6 1 0、乱数依存性決定手段 1 6 2 2、中間データ制御手段 1 6 2 3、記憶装置 1 6 3 0、乱数生成装置 1 6 4 0、および出力装置 1 6 5 0 は、第 1 の

実施の形態や第 7 の実施における同名の構成要素と同様のものである。

【0 1 4 3】

暗号化・復号演算手段 1 6 2 1 は、処理データおよび処理内容を入力とし、中間データ制御手段 1 6 2 3 による乱数依存中間データ変更操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置 1 6 4 0 の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置 1 6 4 0 の出力に依存しない平文を出力する。

【0 1 4 4】

(1 4) 第 1 4 の実施の形態

図 1 7 は、本発明の第 1 4 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【0 1 4 5】

図 1 7 を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置 1 7 1 0 と、暗号化・復号演算手段 1 7 2 1，乱数依存性決定手段 1 7 2 2，および条件分岐制御手段 1 7 2 3 を備える暗号化・復号処理装置 1 7 2 0 と、中間データ記憶部 1 7 3 1 を備える記憶装置 1 7 3 0 と、乱数生成装置 1 7 4 0 と、出力装置 1 7 5 0 とを含んで構成されている。

【0 1 4 6】

本実施の形態に係る暗号化・復号装置は、第 2 の実施の形態に係る暗号化装置の機能と第 8 の実施の形態に係る復号装置の機能とを併有している。ここで、入力装置 1 7 1 0，乱数依存性決定手段 1 7 2 2，条件分岐制御手段 1 7 2 3，記憶装置 1 7 3 0，乱数生成装置 1 7 4 0，および出力装置 1 7 5 0 は、第 2 の実施の形態や第 8 の実施における同名の構成要素と同様のものである。

【0 1 4 7】

暗号化・復号演算手段 1 7 2 1 は、処理データおよび処理内容を入力とし、条件分岐制御手段 1 7 2 3 による乱数依存条件分岐決定操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であっ

た場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置 1 7 4 0 の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置 1 7 4 0 の出力に依存しない平文を出力する。

【0 1 4 8】

(1 5) 第 1 5 の実施の形態

図 1 8 は、本発明の第 1 5 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【0 1 4 9】

図 1 8 を参照すると、本実施の形態に係る暗号化・復号装置は、入力装置 1 8 1 0 と、暗号化・復号演算手段 1 8 2 1，乱数依存性決定手段 1 8 2 2，および遅延制御手段 1 8 2 3 を備える暗号化・復号処理装置 1 8 2 0 と、中間データ記憶部 1 8 3 1 を備える記憶装置 1 8 3 0 と、乱数生成装置 1 8 4 0 と、出力装置 1 8 5 0 とを含んで構成されている。

【0 1 5 0】

本実施の形態に係る暗号化・復号装置は、第 3 の実施の形態に係る暗号化装置の機能と第 9 の実施の形態に係る復号装置の機能とを併有している。ここで、入力装置 1 8 1 0，乱数依存性決定手段 1 8 2 2，遅延制御手段 1 8 2 3，記憶装置 1 8 3 0，乱数生成装置 1 8 4 0，および出力装置 1 8 5 0 は、第 3 の実施の形態や第 9 の実施における同名の構成要素と同様のものである。

【0 1 5 1】

暗号化・復号演算手段 1 8 2 1 は、処理データおよび処理内容を入力とし、遅延制御手段 1 8 2 3 による乱数依存遅延挿入操作に依存して状態を変化させつつ暗号化処理および復号処理を実行し、当該処理内容が暗号化処理であった場合には当該処理データである平文を暗号化した暗号文であって乱数生成装置 1 8 4 0 の出力に依存しない暗号文を出力し、当該処理内容が復号処理であった場合には当該処理データである暗号文を復号した平文であって乱数生成装置 1 8 4 0 の出力に依存しない平文を出力する。

【0 1 5 2】

なお、上述の第 1 3，第 1 4，および第 1 5 の実施の形態に係る暗号化・復号装置においては、入力装置（図 1 6 中の入力装置 1 6 1 0，図 1 7 中の入力装置 1 7 1 0，および図 1 8 中の入力装置 1 8 1 0）から暗号化・復号演算手段（図 1 6 中の暗号化・復号演算手段 1 6 2 1，図 1 7 中の暗号化・復号演算手段 1 7 2 1，および図 1 8 中の暗号化・復号演算手段 1 8 2 1）に暗号化鍵および復号鍵を入力するように構成することも可能である。

【0 1 5 3】

また、上述の第 1 3，第 1 4，および第 1 5 の実施の形態に係る暗号化・復号装置においては、乱数生成装置（図 1 6 中の乱数生成装置 1 6 4 0，図 1 7 中の乱数生成装置 1 7 4 0，および図 1 8 中の乱数生成装置 1 8 4 0）から出力される乱数を、入力装置から暗号化・復号処理装置（図 1 6 中の暗号化・復号処理装置 1 6 2 0，図 1 7 中の暗号化・復号処理装置 1 7 2 0，および図 1 8 中の暗号化・復号処理装置 1 8 2 0）に入力されるデータ（暗号文または平文）そのものまたは当該データに依存したデータとすることも可能である。

【0 1 5 4】

（1 6） 第 1 6 の実施の形態

図 1 9 は、本発明の第 1 6 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【0 1 5 5】

図 1 9 を参照すると、本発明の第 1 6 の実施の形態に係る暗号化・復号装置は、図 1 6 に示した第 1 3 の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体 1 9 0 0 を備える点が異なっている。この記録媒体 1 9 0 0 は、磁気ディスク、半導体メモリ、CD-ROM、その他の記録媒体であってよい。

【0 1 5 6】

暗号化・復号処理プログラムは、記録媒体 1 9 0 0 からコンピュータシステム（入力装置 1 6 1 0，暗号化・復号処理装置 1 6 2 0，記憶装置 1 6 3 0，乱数生成装置 1 6 4 0，および出力装置 1 6 5 0 を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置 1 6 1 0，暗号化・復

号処理装置 1 6 2 0 (暗号化・復号演算手段 1 6 2 1, 乱数依存性決定手段 1 6 2 2, および中間データ制御手段 1 6 2 3), 記憶装置 1 6 3 0 (中間データ記憶部 1 6 3 1), 乱数生成装置 1 6 4 0, および出力装置 1 6 5 0 として制御する。暗号化・復号処理プログラムの制御による入力装置 1 6 1 0, 暗号化・復号処理装置 1 6 2 0, 記憶装置 1 6 3 0, 乱数生成装置 1 6 4 0, および出力装置 1 6 5 0 の動作は、第 1 3 の実施の形態における入力装置 1 6 1 0, 暗号化・復号処理装置 1 6 2 0, 記憶装置 1 6 3 0, 乱数生成装置 1 6 4 0, および出力装置 1 6 5 0 の動作と全く同様になるので、その詳しい説明を割愛する。

【0 1 5 7】

(1 7) 第 1 7 の実施の形態

図 2 0 は、本発明の第 1 7 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【0 1 5 8】

図 2 0 を参照すると、本発明の第 1 7 の実施の形態に係る暗号化・復号装置は、図 1 7 に示した第 1 4 の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体 2 0 0 0 を備える点が異なっている。この記録媒体 2 0 0 0 は、磁気ディスク、半導体メモリ、CD-ROM, その他の記録媒体であってよい。

【0 1 5 9】

暗号化・復号処理プログラムは、記録媒体 2 0 0 0 からコンピュータシステム (入力装置 1 7 1 0, 暗号化・復号処理装置 1 7 2 0, 記憶装置 1 7 3 0, 乱数生成装置 1 7 4 0, および出力装置 1 7 5 0 を備えるコンピュータシステム) に読み込まれ、当該コンピュータシステムの動作を入力装置 1 7 1 0, 暗号化・復号処理装置 1 7 2 0 (暗号化・復号演算手段 1 7 2 1, 乱数依存性決定手段 1 7 2 2, および条件分岐制御手段 1 7 2 3), 記憶装置 1 7 3 0 (中間データ記憶部 1 7 3 1), 乱数生成装置 1 7 4 0, および出力装置 1 7 5 0 として制御する。暗号化・復号処理プログラムの制御による入力装置 1 7 1 0, 暗号化・復号処理装置 1 7 2 0, 記憶装置 1 7 3 0, 乱数生成装置 1 7 4 0, および出力装置 1 7 5 0 の動作は、第 1 4 の実施の形態における入力装置 1 7 1 0, 暗号化・復号

処理装置 1 7 2 0, 記憶装置 1 7 3 0, 乱数生成装置 1 7 4 0, および出力装置 1 7 5 0 の動作と全く同様になるので、その詳しい説明を割愛する。

【0 1 6 0】

(1 8) 第 1 8 の実施の形態

図 2 1 は、本発明の第 1 8 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【0 1 6 1】

図 2 1 を参照すると、本発明の第 1 8 の実施の形態に係る暗号化・復号装置は、図 1 8 に示した第 1 5 の実施の形態に係る暗号化・復号装置に対して、暗号化・復号処理プログラムを記録した記録媒体 2 1 0 0 を備える点が異なっている。この記録媒体 2 1 0 0 は、磁気ディスク、半導体メモリ、CD-ROM, その他の記録媒体であってよい。

【0 1 6 2】

暗号化・復号処理プログラムは、記録媒体 2 1 0 0 からコンピュータシステム（入力装置 1 8 1 0, 暗号化・復号処理装置 1 8 2 0, 記憶装置 1 8 3 0, 乱数生成装置 1 8 4 0, および出力装置 1 8 5 0 を備えるコンピュータシステム）に読み込まれ、当該コンピュータシステムの動作を入力装置 1 8 1 0, 暗号化・復号処理装置 1 8 2 0（暗号化・復号演算手段 1 8 2 1, 乱数依存性決定手段 1 8 2 2, および遅延制御手段 1 8 2 3）, 記憶装置 1 8 3 0（中間データ記憶部 1 8 3 1）, 乱数生成装置 1 8 4 0, および出力装置 1 8 5 0 として制御する。暗号化・復号処理プログラムの制御による入力装置 1 8 1 0, 暗号化・復号処理装置 1 8 2 0, 記憶装置 1 8 3 0, 乱数生成装置 1 8 4 0, および出力装置 1 8 5 0 の動作は、第 1 5 の実施の形態における入力装置 1 8 1 0, 暗号化・復号処理装置 1 8 2 0, 記憶装置 1 8 3 0, 乱数生成装置 1 8 4 0, および出力装置 1 8 5 0 の動作と全く同様になるので、その詳しい説明を割愛する。

【0 1 6 3】

【実施例】

次に、本発明の実施例を、図面を参照して説明する。

【0 1 6 4】

(1) 第1の実施例

図 2 2 および図 2 3 は、本発明の第 1 の実施例を説明するための図である。

【0 1 6 5】

本実施例は、上述の第 1 の実施の形態に係る暗号化装置を、共通鍵暗号 DES (Data Encryption Standard) 対応とするものである。

【0 1 6 6】

なお、DES 暗号については、『「Handbook of Applied Cryptography」(A. Menezes, P. Oorschot, S. Vanstone 著, CRC Press, 1997, ISBN 0-8493-8523-7) pp. 250-259』に詳しく述べられている。

【0 1 6 7】

ここでは、まず、図 2 2 を用いて DES の動作の概要を示す。

【0 1 6 8】

DES は、鍵スケジューリング部 2 2 1 0 と、データ処理部 2 2 2 0 とを備えている。鍵スケジューリング部 2 2 1 0 は、64 ビットの暗号化鍵を入力とし、16 個の 48 ビット中間鍵 $K_1 \sim K_{16}$ を出力する。データ処理部 2 2 2 0 は、初期転置 IP と、最終転置 IP^{-1} と、16 個の F 関数とを備えており、64 ビットの平文と鍵スケジューリング部 2 2 1 0 から出力される 16 個の 48 ビットの中間鍵 $K_1 \sim K_{16}$ を入力とし、64 ビットの暗号文を出力する。ここで IP および IP^{-1} は予め定められているビットの並び替えを行う関数であり、16 個の F 関数は 32 ビットのデータと 48 ビットのデータとを入力とし 32 ビットのデータを出力する予め定められた関数である。

【0 1 6 9】

平文の暗号化は次のように行われる。

【0 1 7 0】

まず、平文は、初期転置 IP が施された後に、上位 32 ビット L_0 と下位 32 ビット R_0 とに分割される。この L_0 および R_0 から、次式に従って $L_1, R_1, L_2, R_2, L_3, R_3, \dots, L_{15}, R_{15}, L_{16}, R_{16}$ が生成される。なお、

上記の L_0 , R_0 , L_1 , R_1 , ... が、図 1 中の中間データ記憶部 1 3 1 内の中間データに該当する。

【 0 1 7 1 】

【 数 1 】

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \oplus F(R_{n-1}, K_n) \quad (\text{但し } \oplus \text{ はビット毎の排他的論理和})$$

【 0 1 7 2 】

ここで、 $n = 1, 2, \dots, 16$ である。なお、上式の記号 F は、DES の F 関数を表している。

【 0 1 7 3 】

DES の 16 個の F 関数は、どれも同じ構造を持ち、32 ビットのデータ R_{n-1} と鍵スケジューリング部 2 2 1 0 より出力される 48 ビットの中間鍵 K_n とを入力とし、32 ビットのデータを出力する。上式を 16 回適用することによって得られた L_{16} を上位 32 ビットとし、 R_{16} を下位 32 ビットとする 64 ビットのデータに対して最終転置 IP^{-1} を施すことによって、64 ビットの暗号文が得られる。

【 0 1 7 4 】

図 2 3 に、本実施例の概念を示す。

【 0 1 7 5 】

図 2 3 において破線で囲まれた部分（図 2 3 中の 2 3 1 0 ~ 2 3 8 0）が、DES の暗号化の過程で必要になる中間データの変化に乱数依存性を持たせている部分（乱数依存性付与部分）である。すなわち、当該乱数依存性付与部分が、図 1 中の中間データ制御手段 1 2 3 により行われる乱数依存中間データ変更操作を表している。

【 0 1 7 6 】

以下に、図 2 2 および図 2 3 を基に、本実施例の構成および動作について説明する。

【 0 1 7 7 】

まず初めに、入力装置である IC カード・リーダー・ライターより平文が入力され

る。平文は初期転置 IP が施された後に、上位 32 ビットと下位 32 ビットとに分けられる。この時点で中間データ制御手段が呼び出される。中間データ制御手段は、乱数生成装置から 2 つの乱数 r_0 および r_1 を受け取り、上位 32 ビットのデータと乱数 r_0 との排他的論理和をとった結果を L_0 に格納し（図 23 の 2310 参照）、下位 32 ビットのデータと乱数 r_1 との排他的論理和をとった結果を R_0 に格納する（図 23 の 2320 参照）。

【0178】

次に、 $n = 1, 2, \dots, 16$ に対し、以下の操作が繰り返される。ただし、以下に現れる r^* の値は次のように定義される。

【0179】

【数 2】

$$r^* = \begin{cases} r_1 & (n = 1, 4, 7, 10, 13, 16 \text{ の時}) \\ r_0 \oplus r_1 & (n = 2, 5, 8, 11, 14 \text{ の時}) \\ r_0 & (n = 3, 6, 9, 12, 15 \text{ の時}) \end{cases}$$

【0180】

まず、 R_{n-1} の値が L_n に複写される。続いて、再び中間データ制御手段が呼び出され、 R_{n-1} と r^* との排他的論理和がとられる（図 23 の 2340, 2360, および 2380 参照）。この排他的論理和の値と K_n とが、 F 関数への入力とされる。以上の手続きにより、 F 関数への入力は R_{n-1} と K_n となり、乱数生成装置から出力される乱数 r^* に依存していないことが確かめられる。

【0181】

F 関数の値が出力されると、中間データ制御手段が呼び出され、再び F 関数の出力と乱数 r^* との排他的論理和がとられる（図 23 の 2330, 2350, および 2370 参照）。さらに、その結果と L_{n-1} との排他的論理和が計算され、計算結果が L_n に格納される。

【0182】

上記操作を 16 回繰り返すことによって得られる L_{16} と r_1 との排他的論理和をとった値を上位 32 ビットとし、 R_{16} と r_0 と r_1 との排他的論理和をとった値を下位 32 ビットとする 64 ビットのデータに、最終転置 IP^{-1} が施された 64 ビットのデータが、暗号文として IC カード・リーダ・ライタを通して出力

される。

【0183】

このとき得られる暗号文は、中間データを操作する乱数 r_0 および r_1 ，遅延時間を制御する乱数，ならびに $S\text{-}b\text{-}o\text{-}x$ の実行順序を決定する乱数のいずれの乱数にも依存しないデータになっている。

【0184】

(2) 第2の実施例

図24，図25，および図26は、本発明の第2の実施例を説明するための図である。

【0185】

本実施例は、上述の第2の実施の形態に係る暗号化装置を、共通鍵暗号 RC5-32/12/16 に適用したものである。

【0186】

なお、RC5-32/12/16 のアルゴリズムの詳細に関しては、上記の「Handbook of Applied Cryptography」の pp. 269-270 に述べられている。

【0187】

ここでは、まず、図24および図25を参照して、RC5-32/12/16 の動作を概説する。

【0188】

RC5-32/12/16 は、図24に示すように、128ビットの暗号化鍵 2420 を用いて64ビットの平文 2410 を64ビットの暗号文 2450 に変換するアルゴリズムである。

【0189】

RC5-32/12/16 は、データ処理部 2430 と、拡大鍵生成部 2440 とを有している。

【0190】

拡大鍵生成部 2440 は、128ビットの暗号化鍵 2420 を入力とし、26個の32ビットの拡大鍵 S_0 ， S_1 ， \dots ， S_{25} を出力する。

【0 1 9 1】

データ処理部 2 4 3 0 は、6 4 ビットの平文 2 4 1 0 と、拡大鍵生成部 2 4 4 0 の出力 S_0 , S_1 , ..., S_{25} とを入力とし、6 4 ビットの暗号文 2 4 5 0 を出力する。

【0 1 9 2】

データ処理部 2 4 3 0 は、次のように動作する。

【0 1 9 3】

まず、入力された 6 4 ビットの平文 2 4 1 0 は、上位 3 2 ビット A と下位 3 2 ビット B とに分割される。次に、A と S_0 との 2^{32} を法とする和（加算）がとられ、その結果が再び A に代入される（図 2 4 の 2 4 3 1 参照）。また、B と S_1 との 2^{32} を法とする和がとられ、その結果が再び B に代入される（図 2 4 の 2 4 3 2 参照）。その後、A および B は、ラウンド関数と呼ばれる変換を 1 2 回適用される。

【0 1 9 4】

暗号文 2 4 5 0 は、ラウンド関数を 1 2 回適用した後の A を上位 3 2 ビットとして持ち、B を下位 3 2 ビットとして持つ 6 4 ビットのデータとなる。

【0 1 9 5】

第 i 回目に適用されるラウンド関数は、A , B , S_{2i} , および S_{2i+1} を入力として A および B のデータの更新を行い、更新された A および B を出力する。

【0 1 9 6】

次に、第 i 回目に適用されるラウンド関数の概要を説明する。

【0 1 9 7】

第 i 回目に適用されるラウンド関数による A および B の更新は、次式に従って行われる。

【0 1 9 8】

【数 3】

$$\begin{aligned} A &= ((A \oplus B) \ll B) + S_{2i} \\ B &= ((B \oplus A) \ll A) + S_{2i+1} \end{aligned}$$

【0 1 9 9】

ここで、「+」は 2^{32} を法とする和を表し、「 $X \ll Y$ 」はXのYビット回転を表している。

【0200】

図25を参照すると、初めに、Aの更新が行われる。まず、入力AはBとビット毎の排他的論理和2510をとられ、その結果がAに再び格納される。次に、Aは、Bビットの左ビット回転2520を施され、その結果が再びAに格納される。最後に、Aと拡大鍵 S_{2i} との 2^{32} を法とする和2530がとられ、その結果が更新後のAの値となる。

【0201】

続いて、Bの更新が行われる。まず、Bは、更新後のAとビット毎の排他的論理和2540をとられ、その結果がBに再び格納される。次に、Bは、Aビットの左ビット回転2550を施され、その結果が再びBに格納される。最後に、Bと拡大鍵 S_{2i+1} との 2^{32} を法とする和2560がとられ、その結果が更新後のBの値となる。

【0202】

本実施例は、入力装置および出力装置としてICカード・リーダー・ライタを、データ記憶装置およびプログラムを格納した記憶媒体として半導体メモリを、暗号化処理装置としてICカードに内蔵されたコンピュータを備えている。暗号化処理装置を実現するコンピュータは、汎用レジスタを5本以上有しており、また当該コンピュータの命令セットは、2つのレジスタR1、R2の算術和、ビット回転、ビット毎の排他的論理和等を計算した結果を必ずR1またはR2に格納するという特徴を有しているものとする。ちなみに、現在使用されているコンピュータの多くは、上記のような特徴を持つ命令セットを有している。

【0203】

次に、図26の流れ図と図24および図25とを基に、本実施例の全体的な動作について詳細に説明する。

【0204】

図26の流れ図において、R1、R2、R3、R4およびR5はデータ幅32ビットの汎用レジスタを表しており、また表記「 $R_i \leftarrow R_i + R_j$ 」は汎用レジ

スタ R_i と R_j とを加算した結果を新たに汎用レジスタ R_i に格納する操作を表している。図 26 中の「 $R_i \leftarrow R_i \lll R_j$ 」等についても同様に解釈するものとする。

【0205】

本実施例は、コンピュータが行う「 $R_i + R_j$ 」および「 $R_i \lll R_j$ 」等のレジスタ間演算の演算結果を R_i および R_j のどちらに格納するかを乱数に依存して変化させることを特徴としている。

【0206】

演算結果の格納先を乱数に依存して変化させることで、電力を測定した場合の消費電力の変化が、汎用レジスタ R_i の値の変化によるものなのか、汎用レジスタ R_j の値の変化によるものなのかを検知することが困難になる。

【0207】

次に、本実施例の動作の詳細な説明を行う。

【0208】

本実施例では、まず初めに、入力装置を通じて暗号化処理装置に平文が格納される（図 26 のステップ D1）。

【0209】

平文が暗号化処理装置に入力されると、暗号化処理装置は汎用レジスタ R_1 に加算（ 2^{32} を法とする和）2431 が終了した後の A の値を格納し、汎用レジスタ R_3 に加算（ 2^{32} を法とする和）2432 が終了した後の B の値を格納する。また、ラウンド関数の実行回数をカウントする変数 r に 1 を格納する（ステップ D2）。

【0210】

次に、暗号化処理装置は、図 25 に示されるラウンド関数の 2510 および 2520 に対応する操作を実行し、さらに汎用レジスタ R_2 に S_{2r} を格納する。

【0211】

この時点で、条件分岐制御手段が呼び出され、 R_2 の保持する S_{2r} の値と R_1 の保持する A の値との和（ 2^{32} を法とする和）2530 をとった計算結果を R_1 および R_2 のどちらに格納するかを乱数の値の偶奇数に応じて変化させる（ステ

ップ D 3 および D 4)。

【0 2 1 2】

図 2 6 のステップ D 4 において乱数の値が奇数であった場合には、R 2 と R 1 との和の計算結果は R 1 に格納される。引き続いて、暗号化演算手段はラウンド関数中の排他的論理和（ビット毎の排他的論理和）2 5 4 0 および左ビット回転 2 5 5 0 を行い、左ビット回転 2 5 5 0 が終了した時点における B の値を R 3 に格納する。

【0 2 1 3】

さらに、R 4 に S_{2r+1} の値を格納し、R 3 と R 4 との和を R 3 に格納する。以上の操作により、ラウンド関数適用後の A および B の値が R 1 および R 3 に格納される（ステップ D 5）。

【0 2 1 4】

ステップ D 5 の処理が終了したことによって 1 回のラウンド関数の処理が終了する。この時点で、現在までに暗号化処理装置が処理したラウンド関数の回数を表す変数 r の値を調べ（ステップ D 7）、r の値が RC 5 - 3 2 / 1 2 / 1 6 が処理すべきラウンド関数の回数である 1 2 と等しかった場合には、出力装置から暗号文を出力して処理を終了する（ステップ D 9）。それ以外の場合には、r に 1 を加え（ステップ D 8）、もう一度ラウンド関数进行处理するためにステップ D 3 に戻る。

【0 2 1 5】

ステップ D 4 において乱数が偶数であった場合には、R 2 と R 1 との和の計算結果は R 2 に格納される。

【0 2 1 6】

引き続いて、暗号化処理装置はラウンド関数の排他的論理和（ビット毎の排他的論理和）2 5 4 0 および左ビット回転 2 5 5 0 を行い、左ビット回転 2 5 5 0 が終了した時点における B の値を R 3 に格納する。

【0 2 1 7】

さらに、R 4 に S_{2r+1} の値を格納し、R 3 と R 4 との和を R 4 に格納する。以上の操作により、ラウンド関数適用後の A および B の値が R 2 および R 4 に格納

される（ステップD 6）。

【0 2 1 8】

次に、ステップD 7の場合と同様に変数 r の値が 1 2 と等しいかどうかを調べ（ステップD 1 4）、等しい場合には出力装置から暗号文を出力して処理を終了する（ステップD 1 6）。それ以外の場合には、 r に 1 を加え（ステップD 1 5）、もう一度ラウンド関数进行处理するためにステップD 1 0に進む。

【0 2 1 9】

ステップD 1 0では、ラウンド関数への入力AおよびBの値がそれぞれR 2およびR 4に格納されている。暗号化処理装置は、図 2 5に示されるラウンド関数の排他的論理和 2 5 1 0および左ビット回転 2 5 2 0を実行し、さらに汎用レジスタR 1に S_{2r} を格納する。この時点で、条件分岐制御手段が呼び出され、R 1の保持する S_{2r} の値とR 2の保持するAの値との和（ 2^{32} を法とする和） 2 5 3 0をとった計算結果をR 1およびR 2のどちらに格納するかを乱数の値の偶奇に応じて変化させる（ステップD 1 0およびD 1 1）。

【0 2 2 0】

図 2 6のステップD 1 1において乱数の値が奇数であった場合には、R 2とR 1との和の計算結果はR 1に格納される。引き続いて、暗号化演算手段はラウンド関数中の排他的論理和 2 5 4 0および左ビット回転 2 5 5 0に対応する操作を行い、左ビット回転 2 5 5 0が終了した時点におけるBの値をR 4に格納する。さらにR 3に S_{2r+1} の値を格納し、R 3とR 4との和をR 3に格納する。以上の操作により、ラウンド関数適用後のAおよびBの値がR 1およびR 3に格納される（ステップD 1 2）。

【0 2 2 1】

ステップD 1 2の処理が終了したことによって1回のラウンド関数の処理が終了する。この時点で、現在までに暗号化処理装置が処理したラウンド関数の回数を表す変数 r の値を調べ（ステップD 7）、 r の値がRC 5 - 3 2 / 1 2 / 1 6が処理すべきラウンド関数の回数である 1 2 と等しかった場合には、出力装置から暗号文を出力して処理を終了する（ステップD 9）。それ以外の場合には、 r に 1 を加え（ステップD 8）、もう一度ラウンド関数进行处理するためにステップ

D 3 に戻る。

【 0 2 2 2 】

ステップ D 1 1 において乱数が偶数であった場合には、R 2 と R 1 との和の計算結果は R 2 に格納される。引き続いて、暗号化処理装置はラウンド関数中の排他的論理和 2 5 4 0 および左ビット回転 2 5 5 0 に対応する操作を行い、左ビット回転 2 5 5 0 が終了した時点における B の値を R 4 に格納する。さらに、R 3 に S_{2r+1} の値を格納し、R 3 と R 4 との和を R 4 に格納する。以上の操作により、ラウンド関数適用後の A および B の値が R 2 および R 4 に格納される（ステップ D 1 3）。

【 0 2 2 3 】

次に、ステップ D 7 の場合と同様に、変数 r の値が 1 2 と等しいかどうかを調べ（ステップ D 1 4）、等しい場合には出力装置から暗号文を出力して処理を終了する（ステップ D 1 6）。それ以外の場合には、r に 1 を加え（ステップ D 1 5）、もう一度ラウンド関数进行处理するためにステップ D 1 0 に戻る。

【 0 2 2 4 】

上記のアルゴリズムにより、乱数生成装置が出力した乱数の値に依存せずに、出力装置には入力平文を暗号化した結果が出力される。

【 0 2 2 5 】

（ 3 ） 第 3 の実施例

図 2 7 および図 2 8 は、本発明の第 3 の実施例を説明するための図である。

【 0 2 2 6 】

本実施例は、上述の第 1 5 の実施の形態に係る暗号化・復号装置を、公開鍵暗号 R S A に適用したものである。

【 0 2 2 7 】

なお、R S A のアルゴリズムに関しては、上記の「Handbook of Applied Cryptography」の pp. 285-291 に詳しく述べられている。

【 0 2 2 8 】

ここでは、まず、R S A の動作の概要を説明する。

【0 2 2 9】

R S A は 5 1 2 ビット程度の 2 つの素数 p , q の積 n と、 $\text{lcm}(p-1, q-1)$ (ただし、 $\text{lcm}(a, b)$ は a と b との最小公倍数を表す) と互いに素である数 e の組 (n, e) とを公開鍵として持ち、法 $\text{lcm}(p-1, q-1)$ の下で $ed = 1$ となるような d を秘密鍵として持つ。

【0 2 3 0】

R S A の暗号化は、次のように行われる。

【0 2 3 1】

M を暗号化したい平文とすると、 M を暗号化した暗号文 C は次式に従って計算される。

【0 2 3 2】

$$C = M^e \bmod n$$

【0 2 3 3】

また、暗号文 C から平文 M を復号する計算は、次式で表される。

【0 2 3 4】

$$M = C^d \bmod n$$

【0 2 3 5】

R S A では、暗号化や復号を高速に行うために、高速な冪乗剰余演算アルゴリズムが必要となる。ここで冪乗剰余演算アルゴリズムとは、 g , e , n を入力として $g^e \bmod n$ を出力するアルゴリズムを指す。

【0 2 3 6】

R S A の実装では、高速な冪乗剰余演算アルゴリズムとして図 2 7 の流れ図で示されるアルゴリズムまたはその改良アルゴリズムを用いることが標準的である。ここでは、図 2 7 の流れ図を基に、高速冪乗剰余演算アルゴリズムの動作の流れを説明する。

【0 2 3 7】

冪乗剰余アルゴリズムでは、まず初めに、 g , e , n が入力される (図 2 7 のステップ E 1)。

【0 2 3 8】

続いて、変数AおよびSに初期値として1およびgをそれぞれ格納する（ステップE2）。

【0239】

続いて、eが0であるかどうかを判定し（ステップE3）、0の場合にはAを出力して処理を終了し、そうでない場合にはeの偶奇を調べ、eが奇数であった場合にはAとSとの積を計算し、その結果を新たに再びAに格納する（ステップE4およびE5）。

【0240】

次に、eの値を2で割ることにより、eの1ビット右シフトを行う（ステップE6）。

【0241】

この段階で再びeが0であるかどうかを判定し（ステップE7）、0である場合にはAを出力して処理を終了し、そうでない場合にはSを二乗して（ステップE8）、ステップE3に戻る。

【0242】

eの二進数表現を (b_1, b_2, \dots, b_t) とすると（ただし、 b_1 が最上位ビット、 b_t が最下位ビット）、図27の流れ図においてステップE7をi回通過した時点でのAの値は、二進数表現が (b_1, b_2, \dots, b_i) となるような数 e_i に対して $g^{e_i} \bmod n$ となっている。

【0243】

アルゴリズムの構成法により、図27で示されるアルゴリズムではeのビット長tに対してアルゴリズム終了時までステップE7を通過する回数は必ずt回となるので、アルゴリズム終了時のAの値は $g^e \bmod n$ となり冪乗剰余演算が計算されていることが分かる。

【0244】

しかし、上記のようなアルゴリズムを用いて冪乗剰余演算を実現する場合には、次のような問題が生じる。図27のステップE4をi回通過した後にステップE5が実行される必要十分条件は、eの右からiビット目が1であることとなる。この時、上記のアルゴリズムを実装した装置の実行中に当該装置が消費する電

力を測定することにより、当該装置内で実行されている命令の特定が可能である
とすると、RSA暗号文の復号時における当該装置の消費電力を測定することによりRSAの秘密鍵 d を特定することが可能になってしまう。

【0245】

次に、図27の流れ図および図28を参照して本実施例を詳細に説明する。

【0246】

本実施例の暗号化・復号装置における暗号化・復号処理装置2820は、暗号化・復号演算手段2821と、乱数依存性決定手段2822と、遅延制御手段2823とを備えており、次のように動作する。

【0247】

暗号化・復号演算手段2821は、2つの相異なる数 a 、 b と法 n とを入力とし、 $a \cdot b \bmod n$ を計算する乗算器28211と、1つの数 a と法 n とを入力とし、 $a^2 \bmod n$ を計算する二乗演算器28212とを備えている。

【0248】

暗号化・復号演算手段2821は、暗号化と復号との2つの機能を有しており、暗号化を行う場合には入力装置2810から通信相手の公開鍵 e 、 n_1 と送信したい平文 M とを入力し、図27の流れ図と同様な動作を行うことによって、暗号文 $M^e \bmod n_1$ を計算し、その計算結果を出力装置2850より出力する。また、復号を行う場合には、入力装置2810から本人の秘密鍵 d と本人の公開鍵 n_2 および受信した暗号文 C とを入力し、図27の流れ図と同様な動作を行うことによって、平文 $C^d \bmod n_2$ を計算し、その計算結果を出力装置2850より出力する。

【0249】

図28中の暗号化・復号演算手段2821の動作が図27の流れ図と異なる点は、図28中の暗号化・復号演算手段2821は、図27のステップE8からステップE3に戻る時点で乱数依存性決定手段2822によって遅延時間決定要求が遅延制御手段2823に出力される点にある。

【0250】

遅延制御手段2823は、暗号化演算手段2821と同様に、乗算器2823

1 と、二乗演算器 2 8 2 3 2 とを備えており、乱数依存性決定手段 2 8 2 2 より遅延時間決定要求が出されると、乱数生成装置 2 8 4 0 に対して乱数要求信号を 2 度送り、2 つの乱数 r_1 , r_2 を得る。

【0 2 5 1】

r_1 と r_2 とを受け取った遅延制御手段 2 8 2 3 は、 r_1 の最下位ビットが 0 であるか否かを判定し、0 であった場合には遅延挿入のために、二乗演算器 2 8 2 3 2 を用いて r_2 の二乗の計算を行い、再び暗号化・復号演算手段 2 8 2 1 に処理を移す。一方、 r_1 の最下位ビットが 1 であった場合には、遅延挿入のために、遅延制御手段 2 8 2 3 は、乗算器 2 8 2 3 1 を用いて r_1 と r_2 との積を計算した後に、二乗演算器 2 8 2 3 2 を用いて乗算器 2 8 2 3 1 の計算結果である $r_1 \cdot r_2$ の二乗を計算し、再び暗号化・復号演算手段 2 8 2 1 に処理を移す。

【0 2 5 2】

【発明の効果】

以上説明したように、本発明の暗号化装置、復号装置、および暗号化・復号装置によると、データの暗号化や復号を行う際に当該装置の消費電力を測定することによって暗号化鍵や復号鍵等の秘密情報を得る暗号解析法（電力解析や電力差分解析等の消費電力の測定による暗号解析法）の適用が困難になるという効果が生じる。

【0 2 5 3】

以上のような効果が生じる理由を、以下に述べる。

【0 2 5 4】

電力解析や電力差分解析等の消費電力の測定による暗号解析が成功するためには、第 1 に暗号化装置や復号装置がデータの暗号化や復号を行っている際に消費する電力と当該装置内で行われている暗号化操作や復号操作との間に密接な関連があること、第 2 に暗号化装置や復号装置が特定の暗号化操作や復号操作を行っている時刻が容易に検知できること、の 2 点が必要条件となる。

【0 2 5 5】

本発明では、中間データ制御手段によって暗号化や復号を行う際に必要となる

中間データが乱数に依存して変化したまま暗号装置や復号装置内で暗号化操作や復号操作が行われるため、当該装置が消費した電力の変化が実際の暗号化操作や復号操作によって生じたものであるのか、乱数の影響によって生じたものであるのかの判断が困難になっている。したがって、暗号化装置や復号装置の消費電力と当該装置内で行われている暗号化操作や復号操作との間の関連が検知しづらくなるため、電力解析や電力差分解析が成功するための第 1 の必要条件が成立しなくなる。

【0 2 5 6】

さらに、本発明では、条件分岐制御手段によって、順序を入れ替えることが可能であるような操作の順序（実行順序）の決定や、どの操作を実行しても暗号化や復号の結果が変化しないような複数の操作の選択肢の中から実際に実行される操作を選択することを、乱数に依存して行っている。また、遅延制御手段によって、暗号化や復号の操作の途中で、適宜乱数に依存した時間の遅延が挿入される。それらのために、特定の暗号化や復号の操作が実行される時刻が、乱数によって変化することになる。したがって、電力解析や電力差分解析が成功するための第 2 の必要条件が成立しなくなる。

【0 2 5 7】

以上により、電力解析や電力差分解析の成功に必要な 2 つの条件が成立しなくなるため、暗号化装置や復号装置の消費電力を測定することで秘密情報を得るという暗号解析法が困難になる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図 2】

図 1 に示す暗号化装置の処理を示す流れ図である。

【図 3】

本発明の第 2 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図 4】

図 3 に示す暗号化装置の処理を示す流れ図である。

【図 5】

本発明の第 3 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図 6】

図 5 に示す暗号化装置の処理を示す流れ図である。

【図 7】

本発明の第 4 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図 8】

本発明の第 5 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図 9】

本発明の第 6 の実施の形態に係る暗号化装置の構成を示すブロック図である。

【図 1 0】

本発明の第 7 の実施の形態に係る復号装置の構成を示すブロック図である。

【図 1 1】

本発明の第 8 の実施の形態に係る復号装置の構成を示すブロック図である。

【図 1 2】

本発明の第 9 の実施の形態に係る復号装置の構成を示すブロック図である。

【図 1 3】

本発明の第 1 0 の実施の形態に係る復号装置の構成を示すブロック図である。

【図 1 4】

本発明の第 1 1 の実施の形態に係る復号装置の構成を示すブロック図である。

【図 1 5】

本発明の第 1 2 の実施の形態に係る復号装置の構成を示すブロック図である。

【図 1 6】

本発明の第 1 3 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図 1 7】

本発明の第 1 4 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図 1 8】

本発明の第 1 5 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図 1 9】

本発明の第 1 6 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図 2 0】

本発明の第 1 7 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図 2 1】

本発明の第 1 8 の実施の形態に係る暗号化・復号装置の構成を示すブロック図である。

【図 2 2】

本発明の第 1 の実施例を説明するための図（D E S の構成を示すブロック図）である。

【図 2 3】

本発明の第 1 の実施例を説明するための図（当該実施例の構成を示すブロック図）である。

【図 2 4】

本発明の第 2 の実施例を説明するための図（R C 5 - 3 2 / 1 2 / 1 6 の構成を示すブロック図）である。

【図 2 5】

本発明の第 2 の実施例を説明するための図（RC 5 - 3 2 / 1 2 / 1 6 のラウンド関数の構成を示すブロック図）である。

【図 2 6】

本発明の第 2 の実施例を説明するための図（当該実施例の動作を示す流れ図）である。

【図 2 7】

本発明の第 3 の実施例を説明するための図（高速冪乗剰余演算の動作を示す流れ図）である。

【図 2 8】

本発明の第 3 の実施例を説明するための図（当該実施例の構成を示すブロック図）である。

【符号の説明】

1 1 0, 3 1 0, 5 1 0, 1 0 1 0, 1 1 1 0, 1 2 1 0, 1 6 1 0, 1 7 1 0, 1 8 1 0, 2 8 1 0 入力装置

1 2 0, 3 2 0, 5 2 0 暗号化处理装置

1 2 1, 3 2 1, 5 2 1 暗号化演算手段

1 2 2, 3 2 2, 5 2 2, 1 0 2 2, 1 1 2 2, 1 2 2 2, 1 6 2 2, 1 7 2 2, 1 8 2 2, 2 8 2 2 乱数依存性決定手段

1 2 3, 1 0 2 3, 1 6 2 3 中間データ制御手段

1 3 0, 3 3 0, 5 3 0, 1 0 3 0, 1 1 3 0, 1 2 3 0, 1 6 3 0, 1 7 3 0, 1 8 3 0, 2 8 3 0 記憶装置

1 3 1, 3 3 1, 5 3 1, 1 0 3 1, 1 1 3 1, 1 2 3 1, 1 6 3 1, 1 7 3 1, 1 8 3 1, 2 8 3 1 中間データ記憶部

1 4 0, 3 4 0, 5 4 0, 1 0 4 0, 1 1 4 0, 1 2 4 0, 1 6 4 0, 1 7 4 0, 1 8 4 0, 2 8 4 0 乱数生成装置

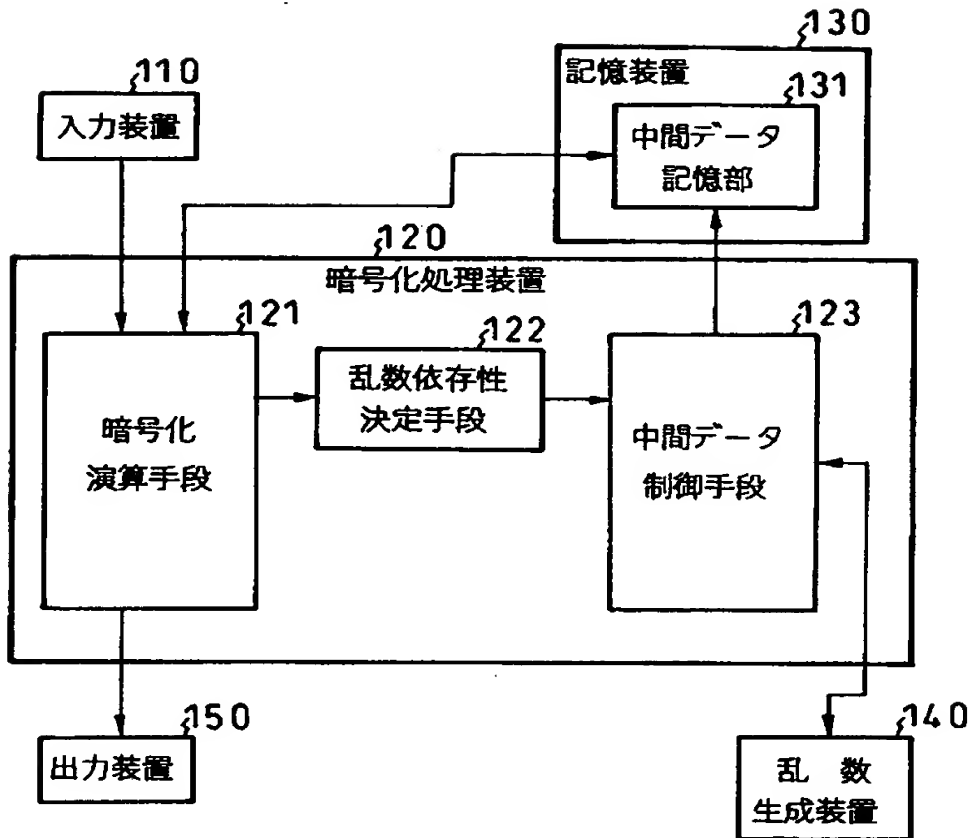
1 5 0, 3 5 0, 5 5 0, 1 0 5 0, 1 1 5 0, 1 2 5 0, 1 6 5 0, 1 7 5 0, 1 8 5 0, 2 8 5 0 出力装置

3 2 3, 1 1 2 3, 1 7 2 3 条件分岐制御手段

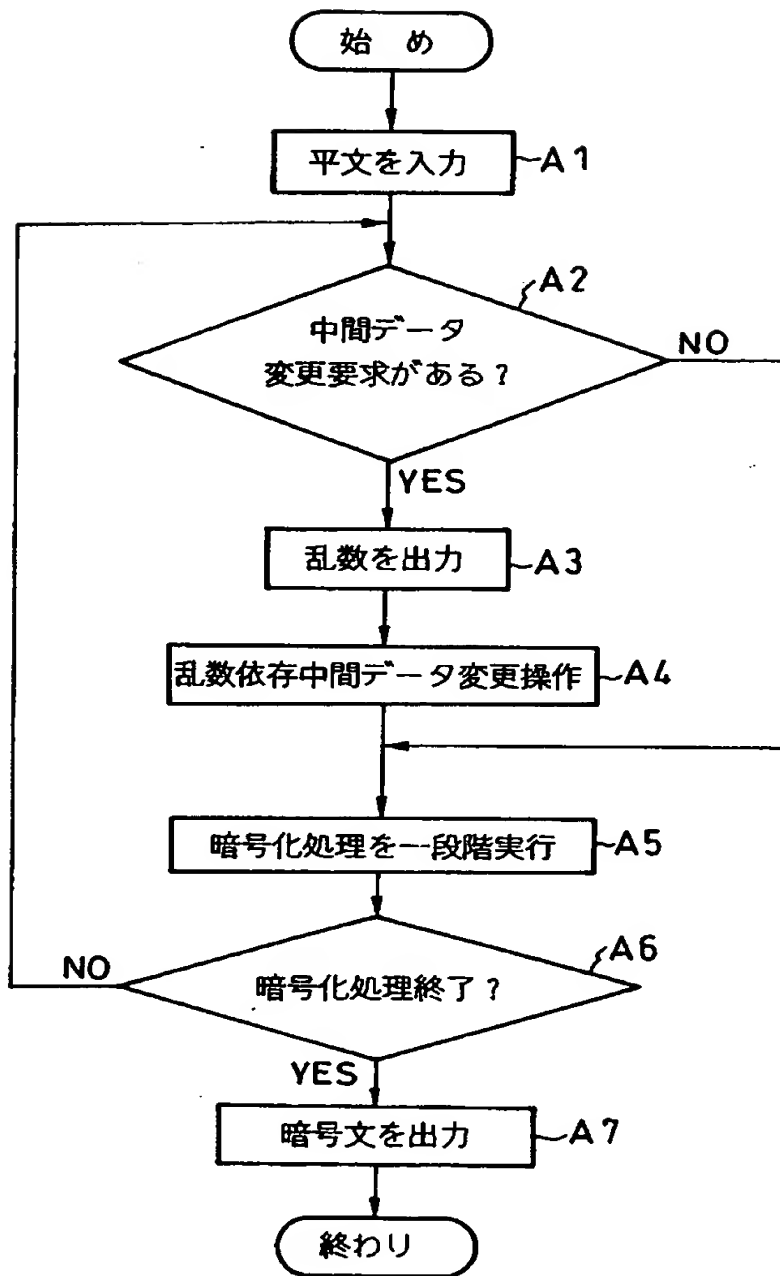
5 2 3, 1 2 2 3, 1 8 2 3, 2 8 2 3 遅延制御手段
7 0 0, 8 0 0, 9 0 0, 1 3 0 0, 1 4 0 0, 1 5 0 0, 1 9 0 0, 2 0 0
0, 2 1 0 0 記録媒体
1 0 2 0, 1 1 2 0, 1 2 2 0 復号処理装置
1 0 2 1, 1 1 2 1, 1 2 2 1 復号演算手段
1 6 2 0, 1 7 2 0, 1 8 2 0, 2 8 2 0 暗号化・復号処理装置
1 6 2 1, 1 7 2 1, 1 8 2 1, 2 8 2 1 暗号化・復号演算手段
2 2 1 0 鍵スケジューリング部
2 2 2 0, 2 4 3 0 データ処理部
2 3 1 0, 2 3 2 0, 2 3 3 0, 2 3 4 0, 2 3 5 0, 2 3 6 0, 2 3 7 0,
2 3 8 0 乱数依存性付与部分
2 4 1 0 平文
2 4 2 0 暗号化鍵
2 4 3 1, 2 4 3 2, 2 5 3 0, 2 5 6 0 2^{32} を法とする和
2 4 4 0 拡大鍵生成部
2 4 5 0 暗号文
2 5 1 0, 2 5 4 0 ビット毎の排他的論理和
2 5 2 0, 2 5 5 0 左ビット回転
2 8 2 1 1, 2 8 2 3 1 乗算器
2 8 2 1 2, 2 8 2 3 2 二乗演算器

【書類名】 図面

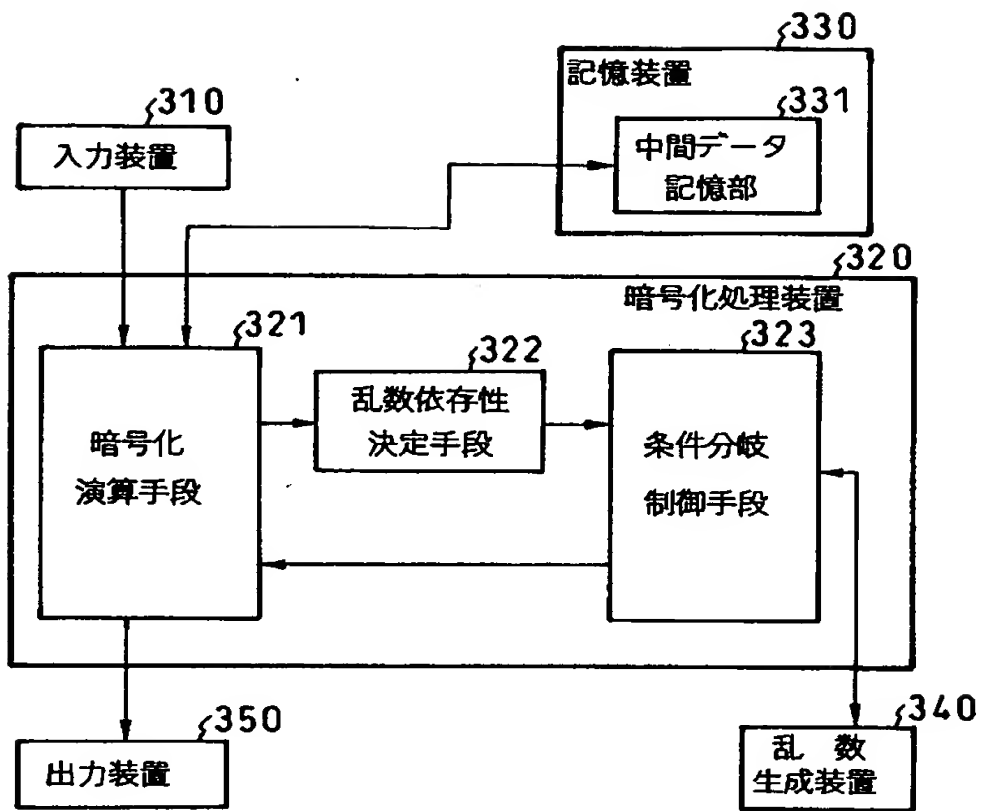
【図 1】



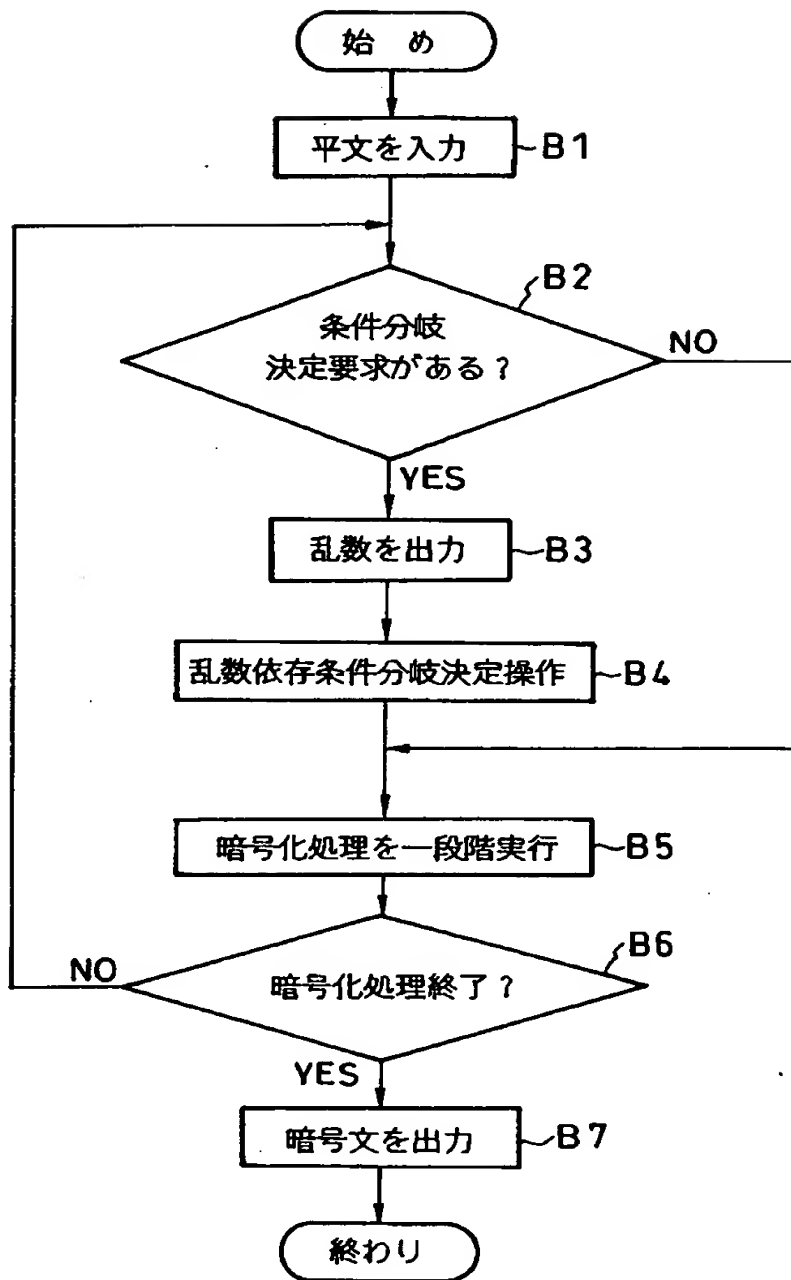
【図 2】



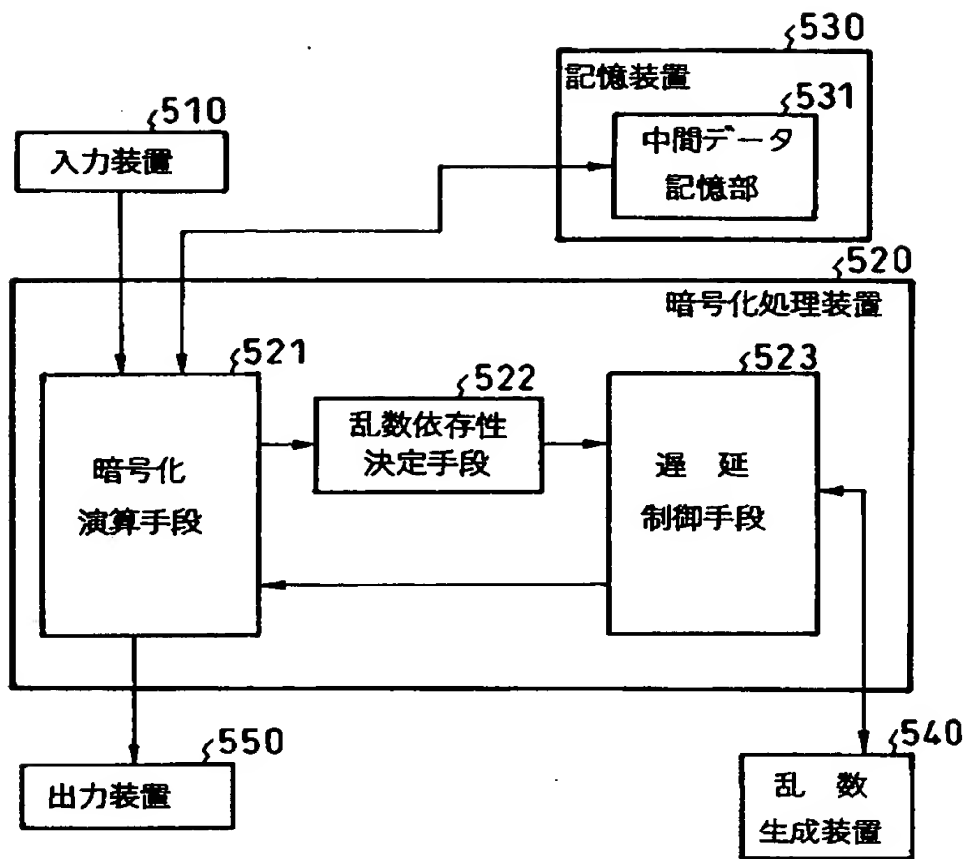
【図 3】



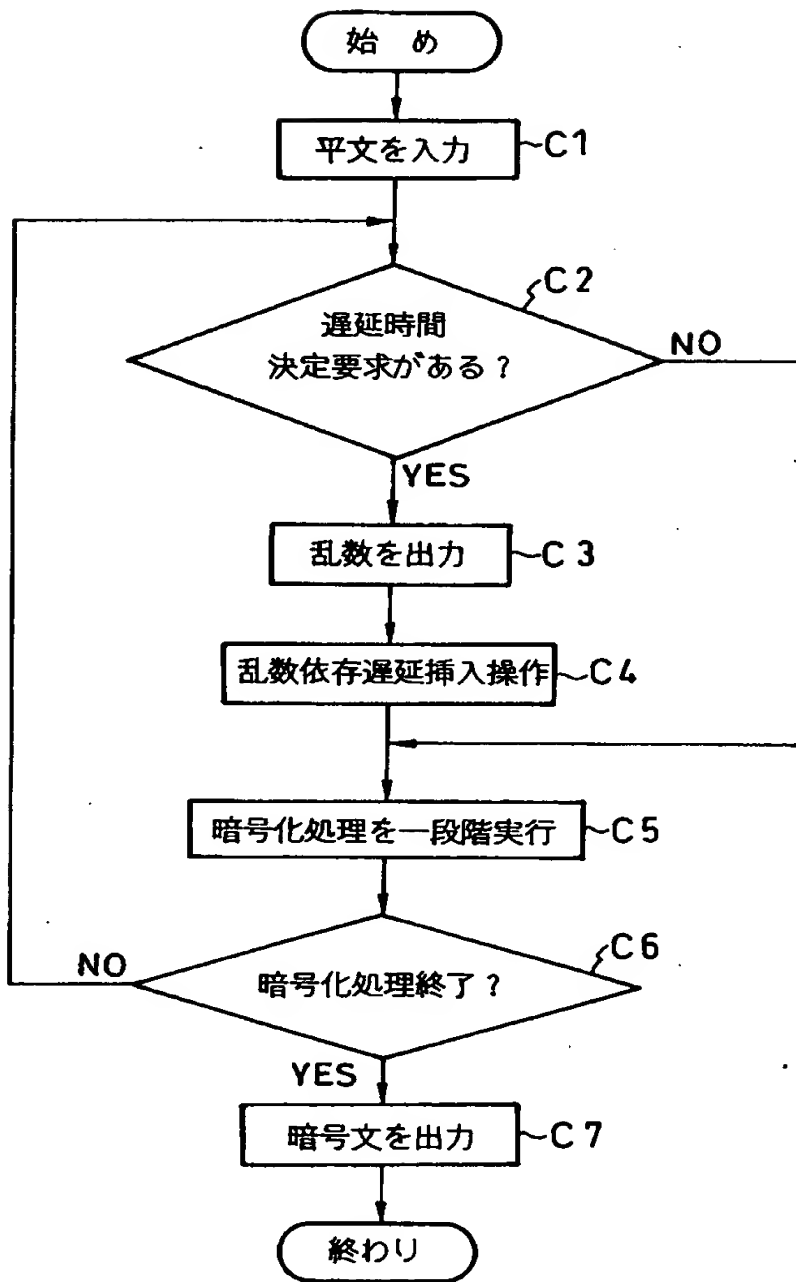
【図 4】



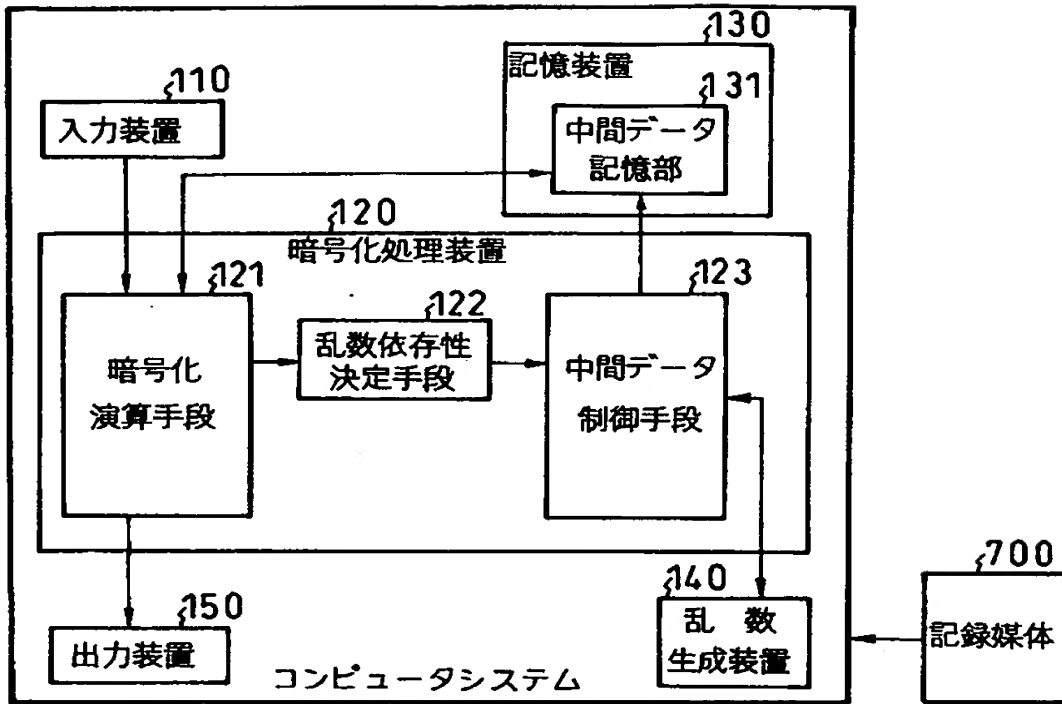
【図 5】



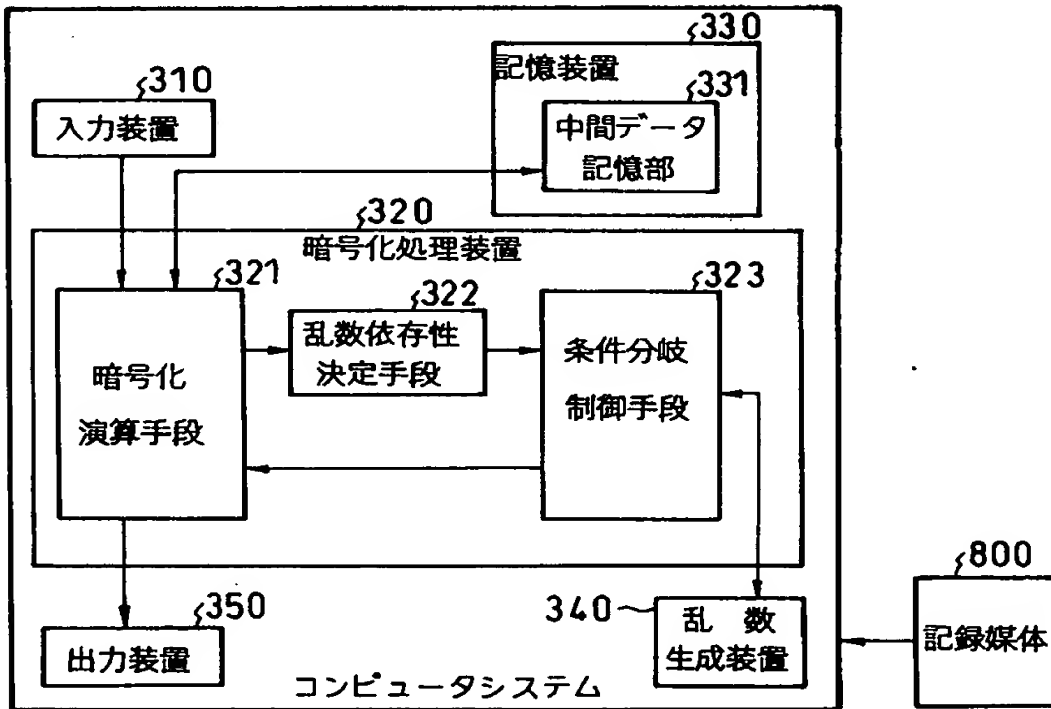
【図 6】



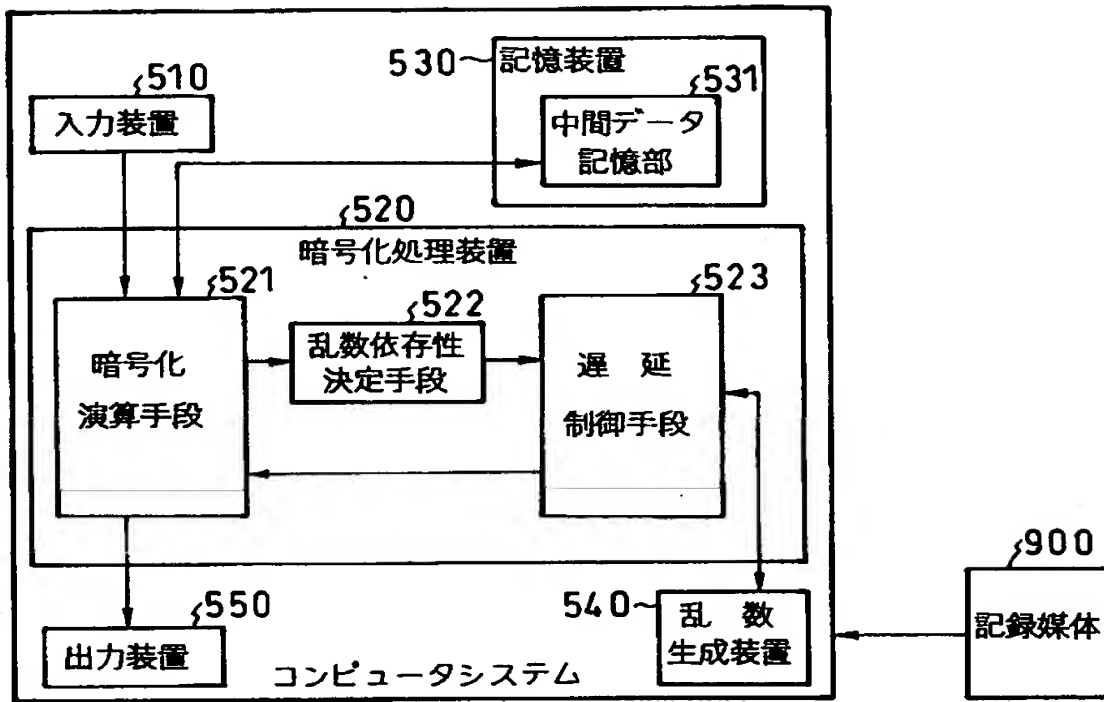
【図 7】



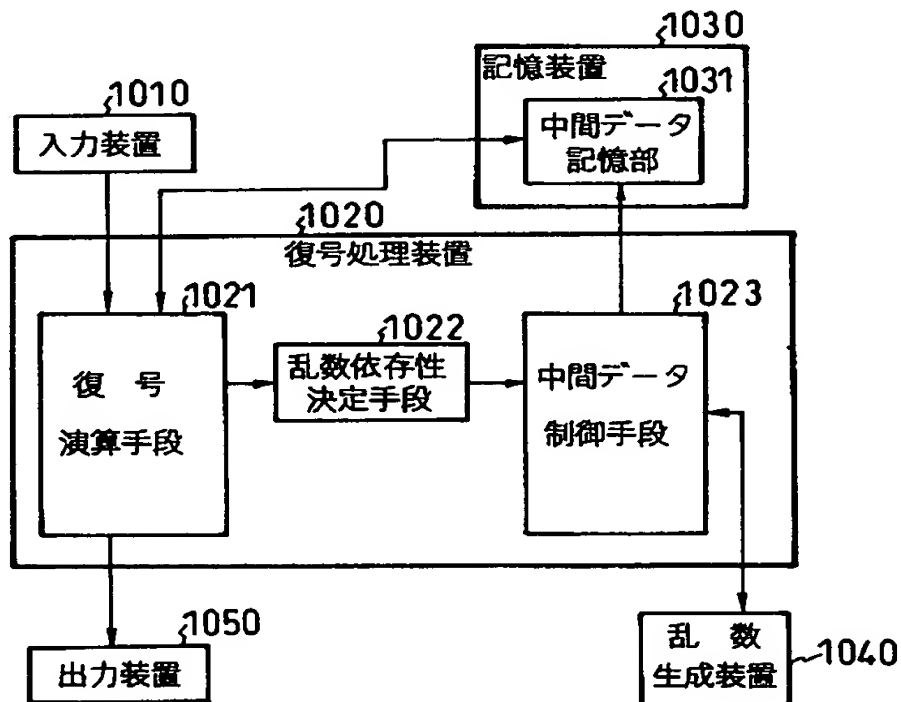
【図 8】



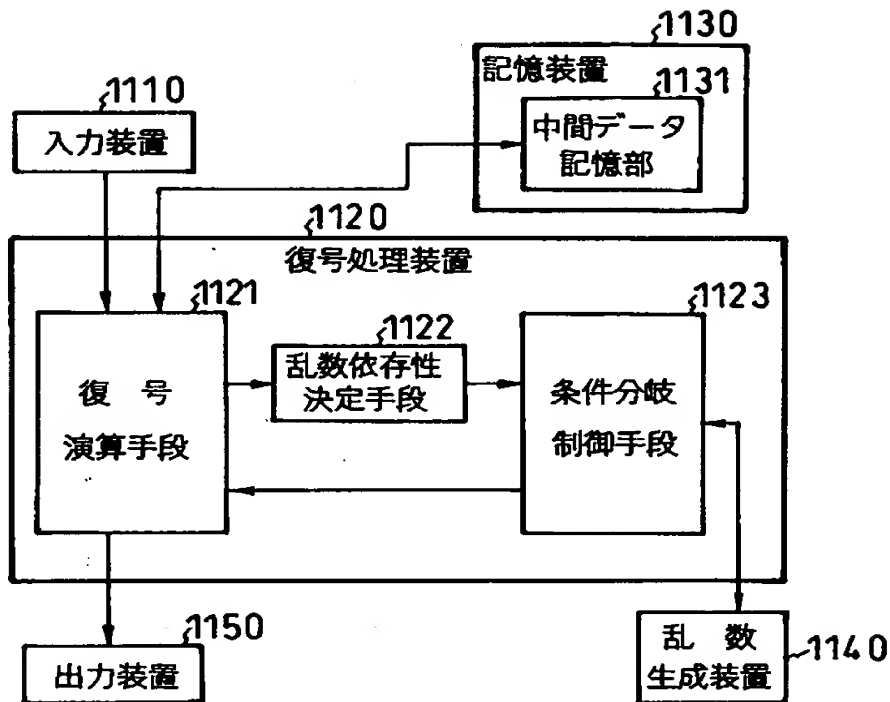
【図 9】



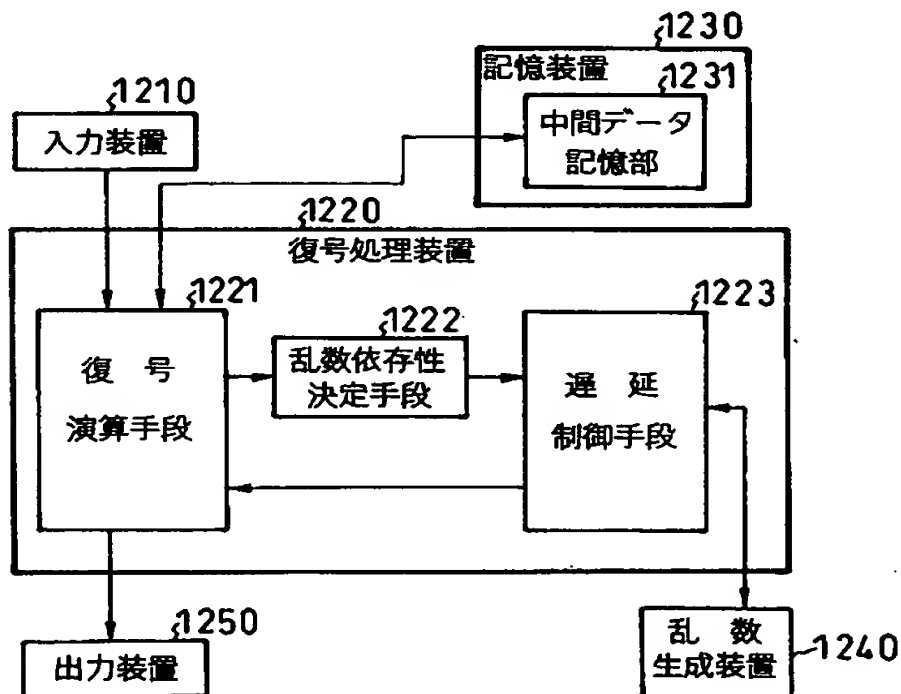
【図 10】



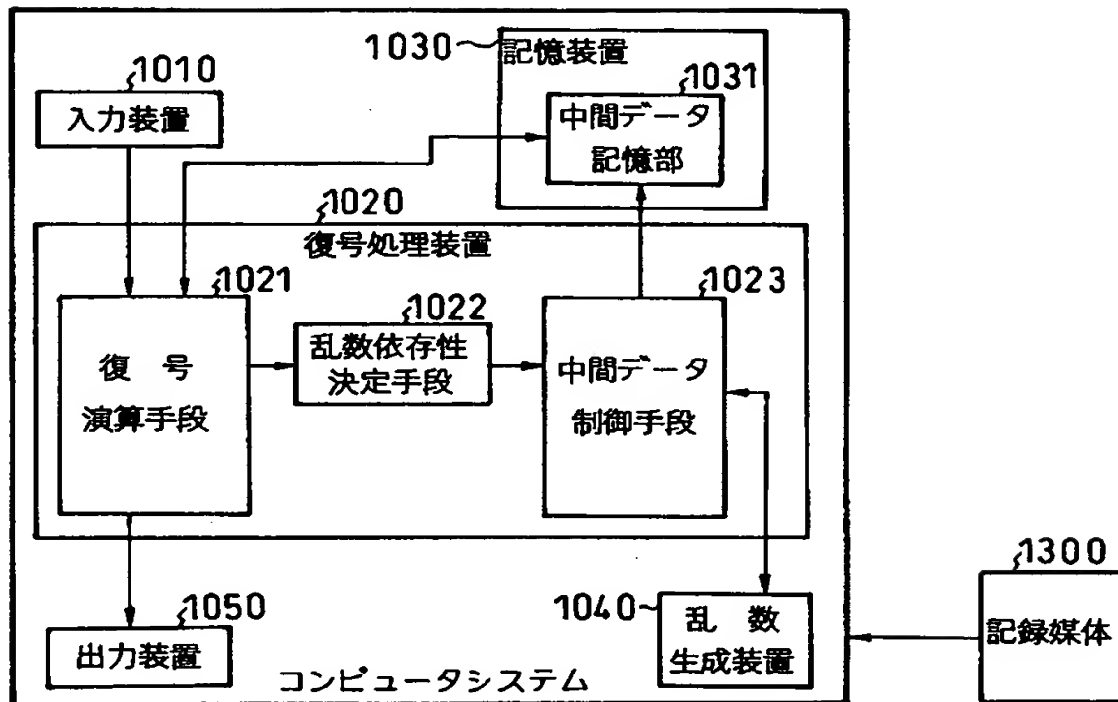
【図 1 1】



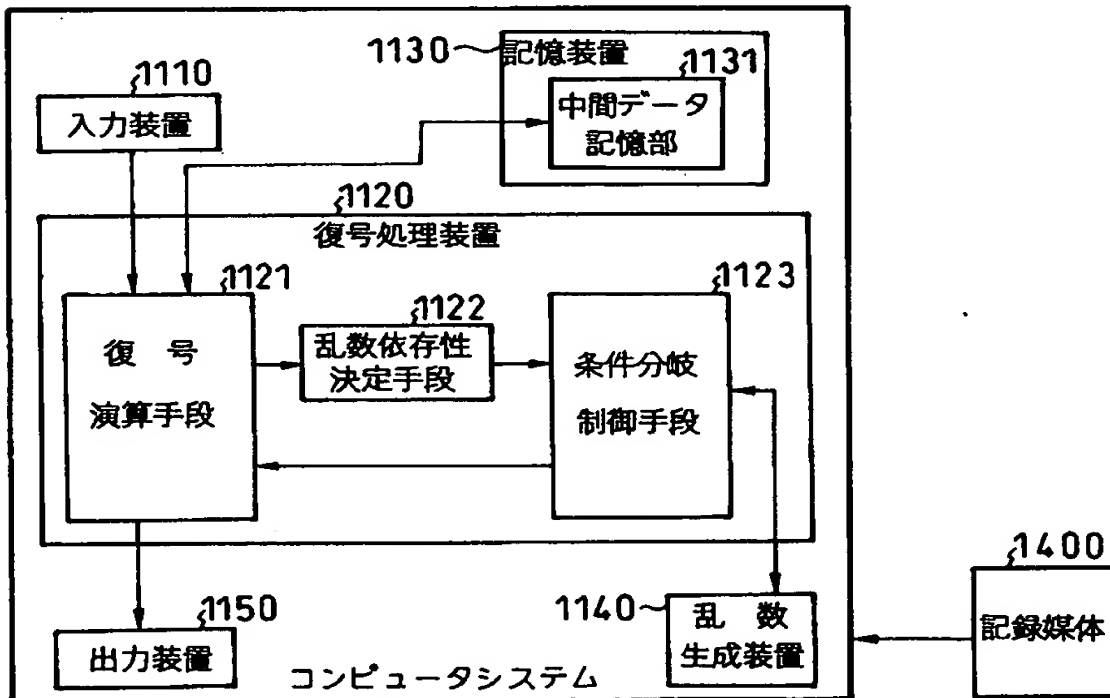
【図 1 2】



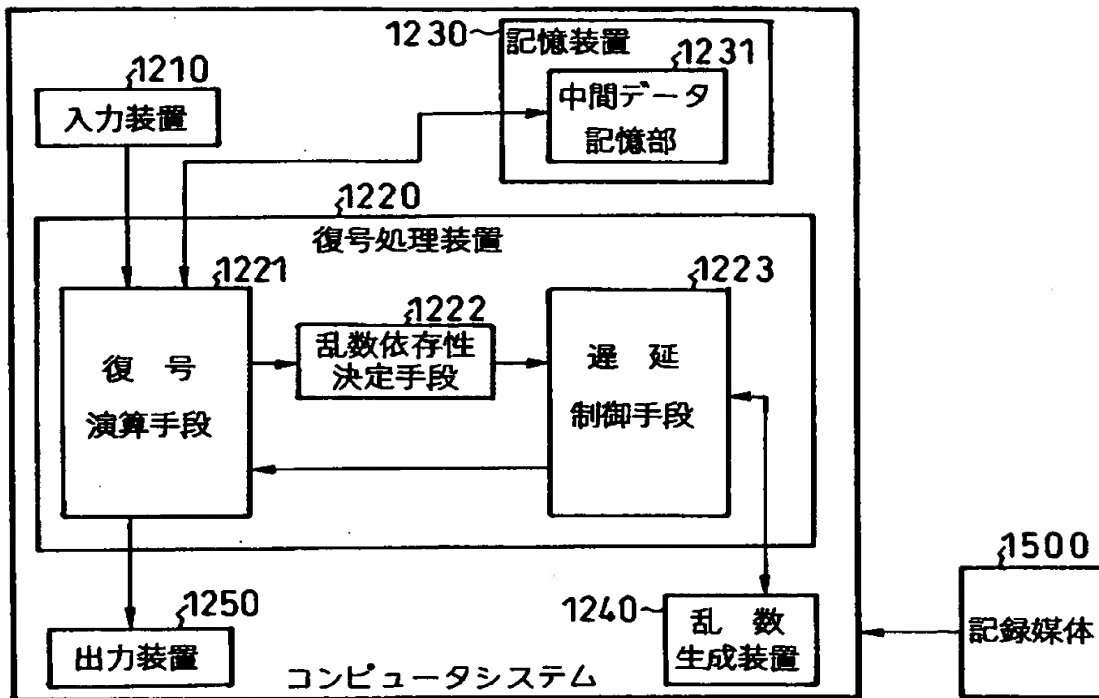
【図 1 3】



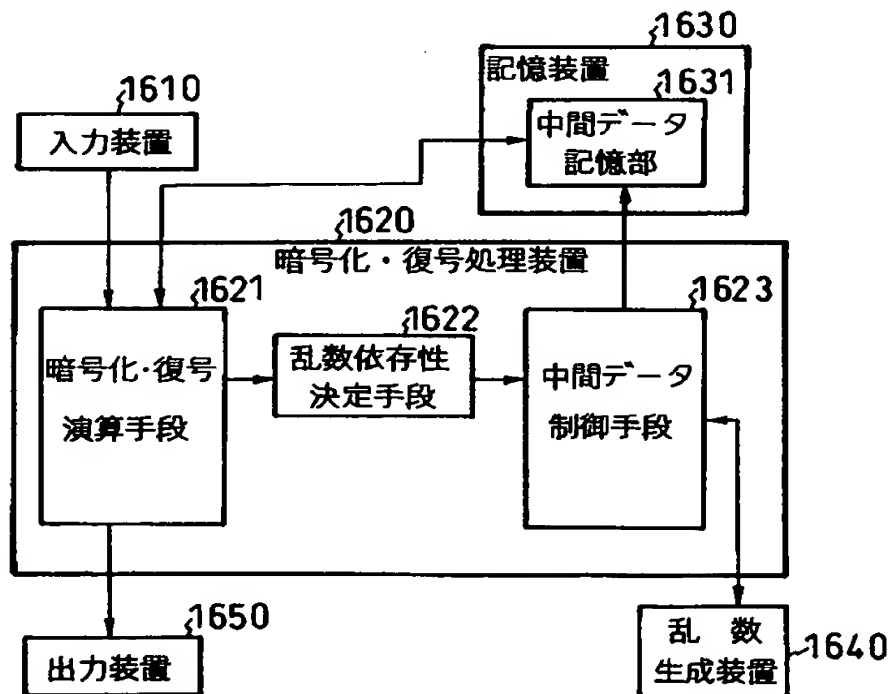
【図 1 4】



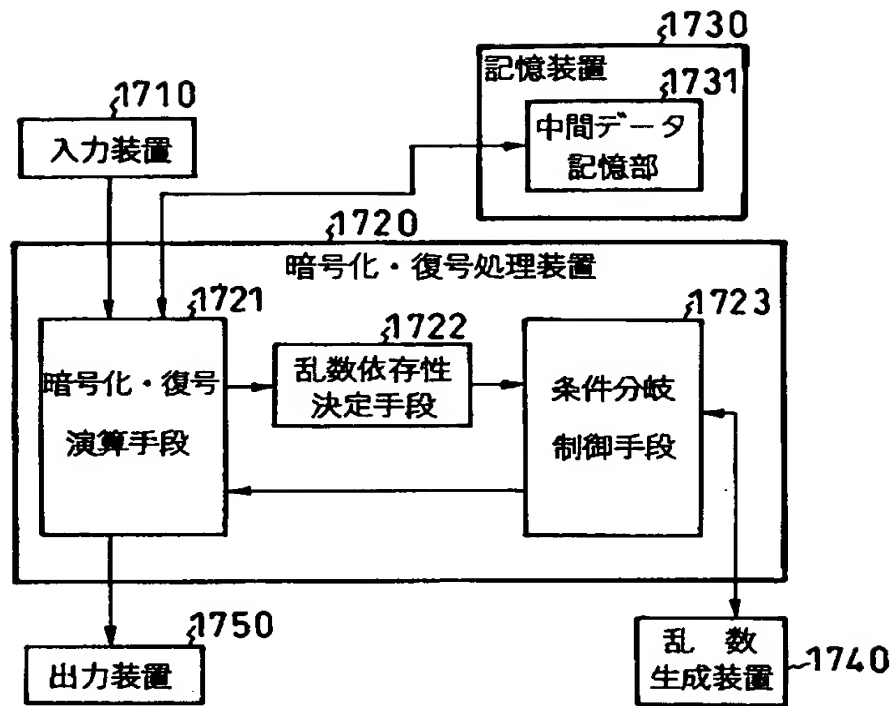
【図 1 5】



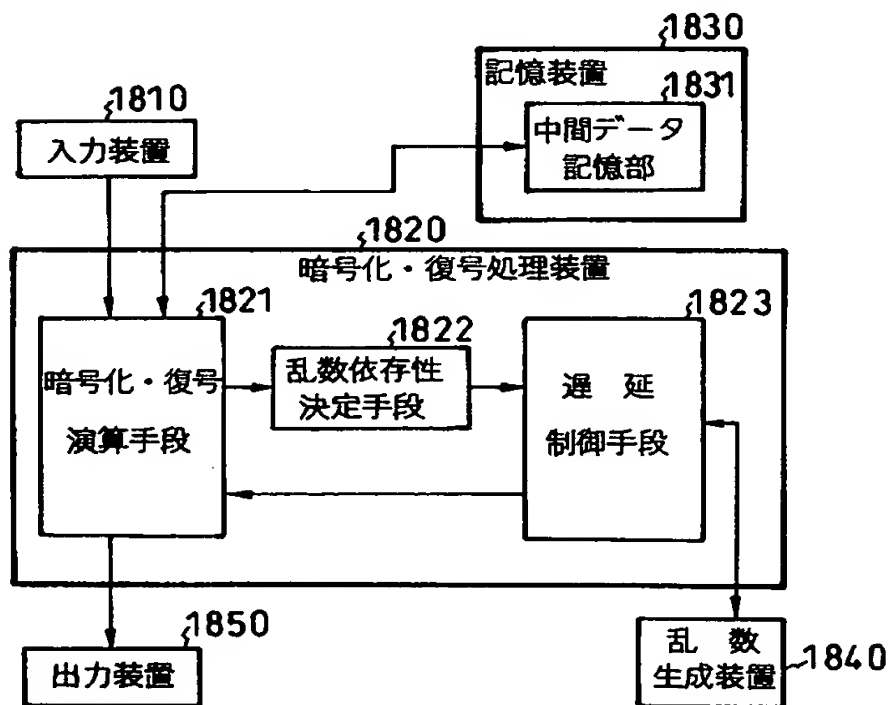
【図 1 6】



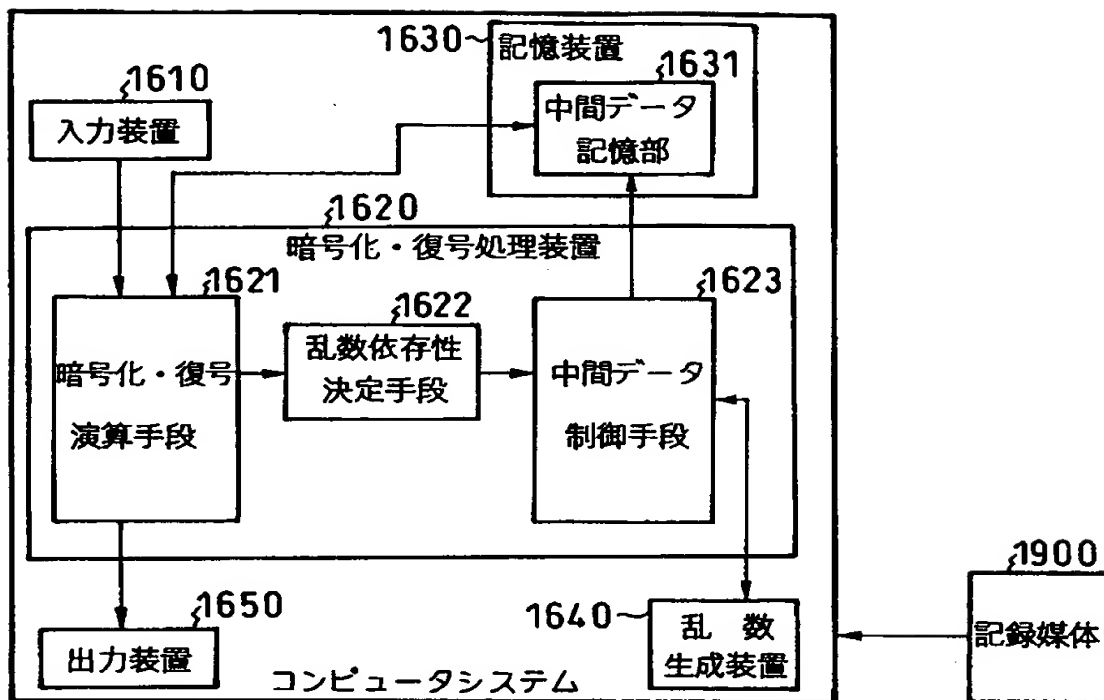
【図 1 7】



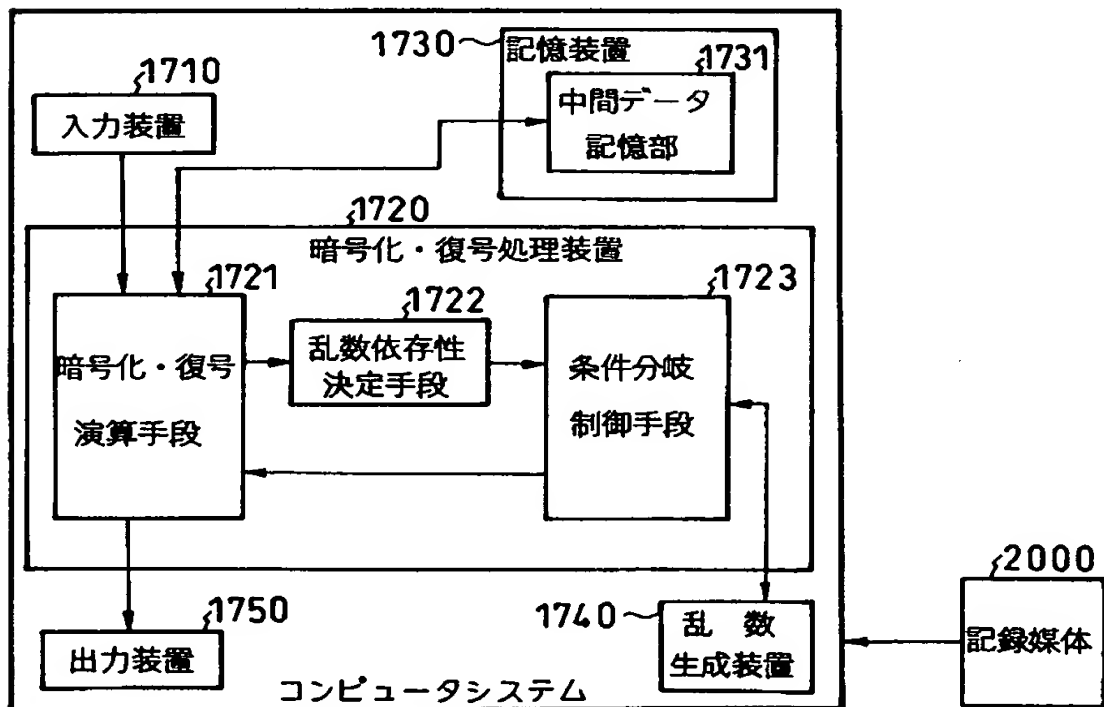
【図 1 8】



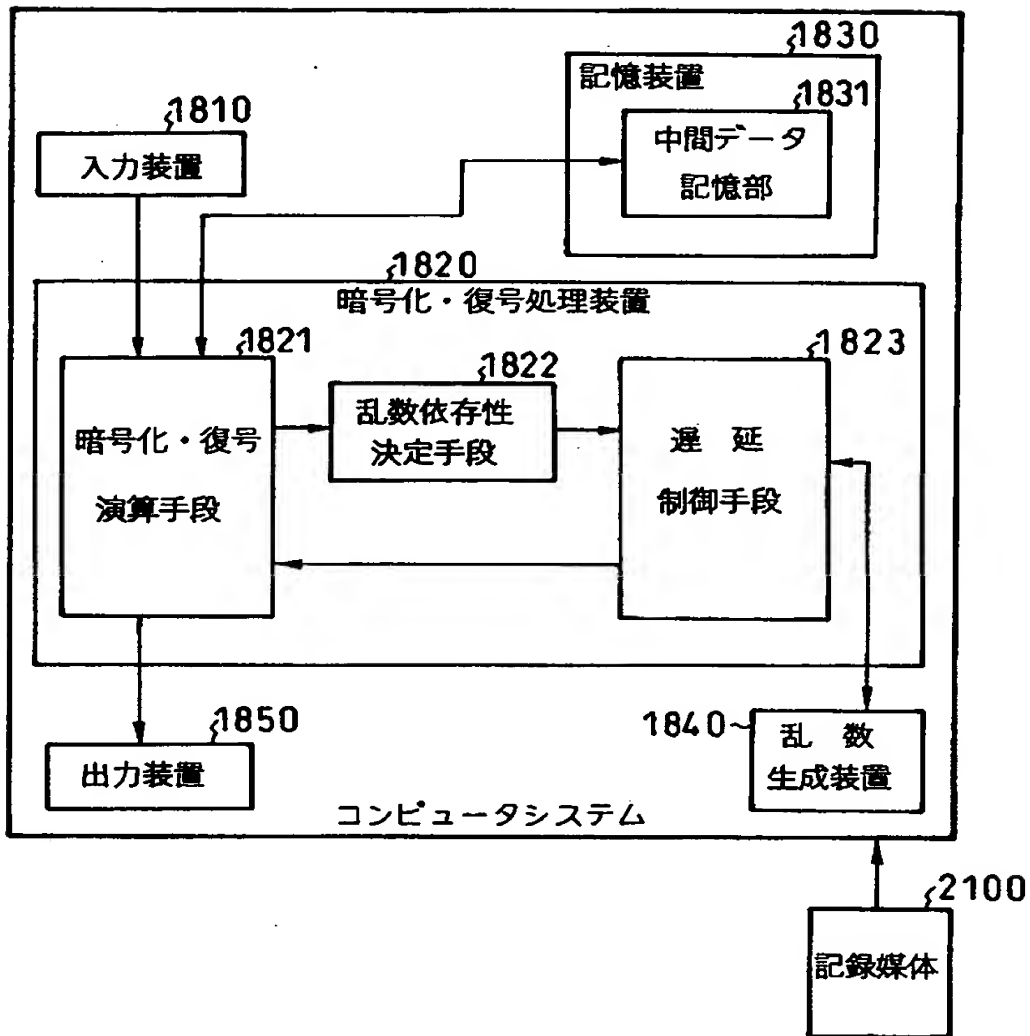
【図 1 9】



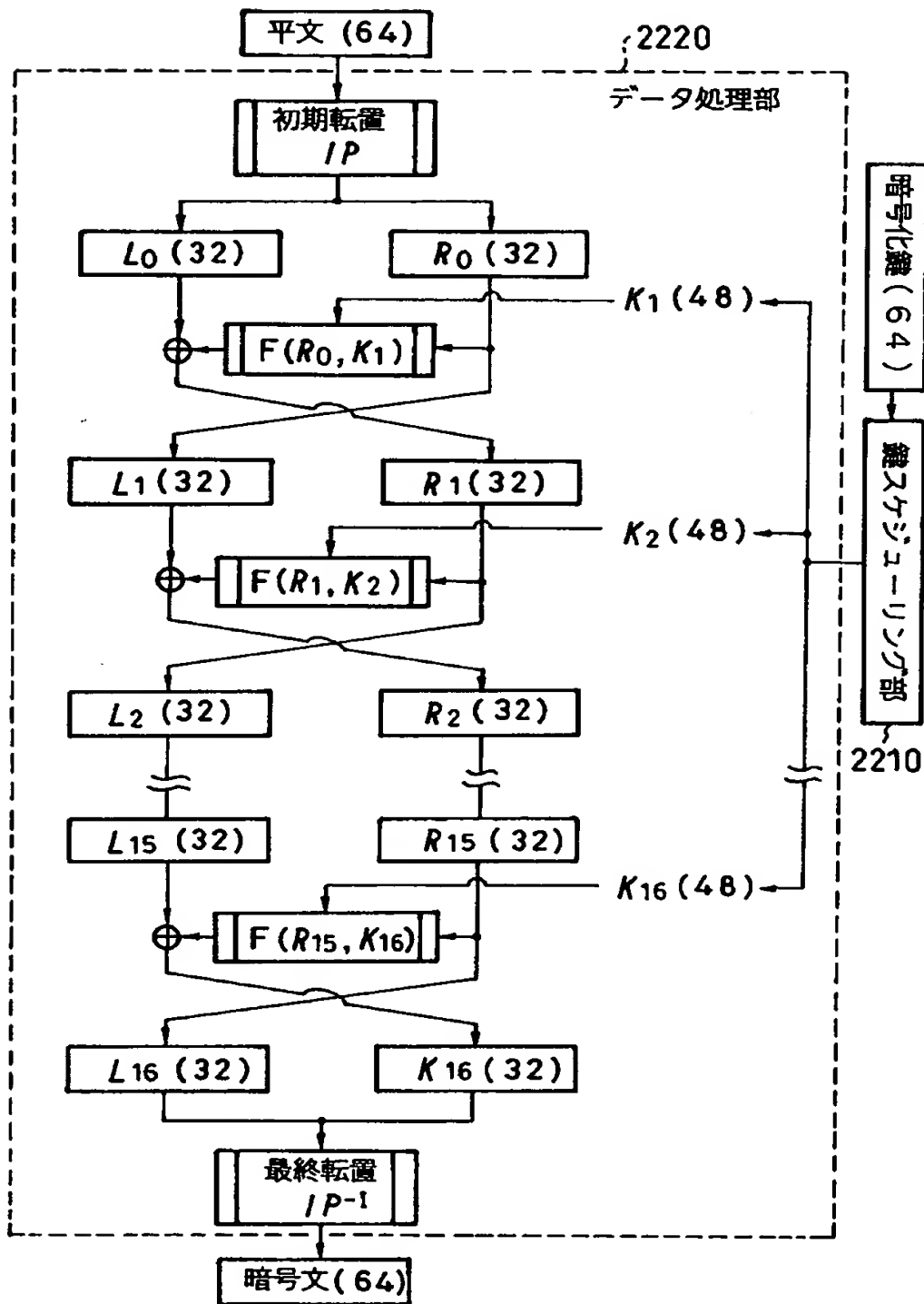
【図 2 0】



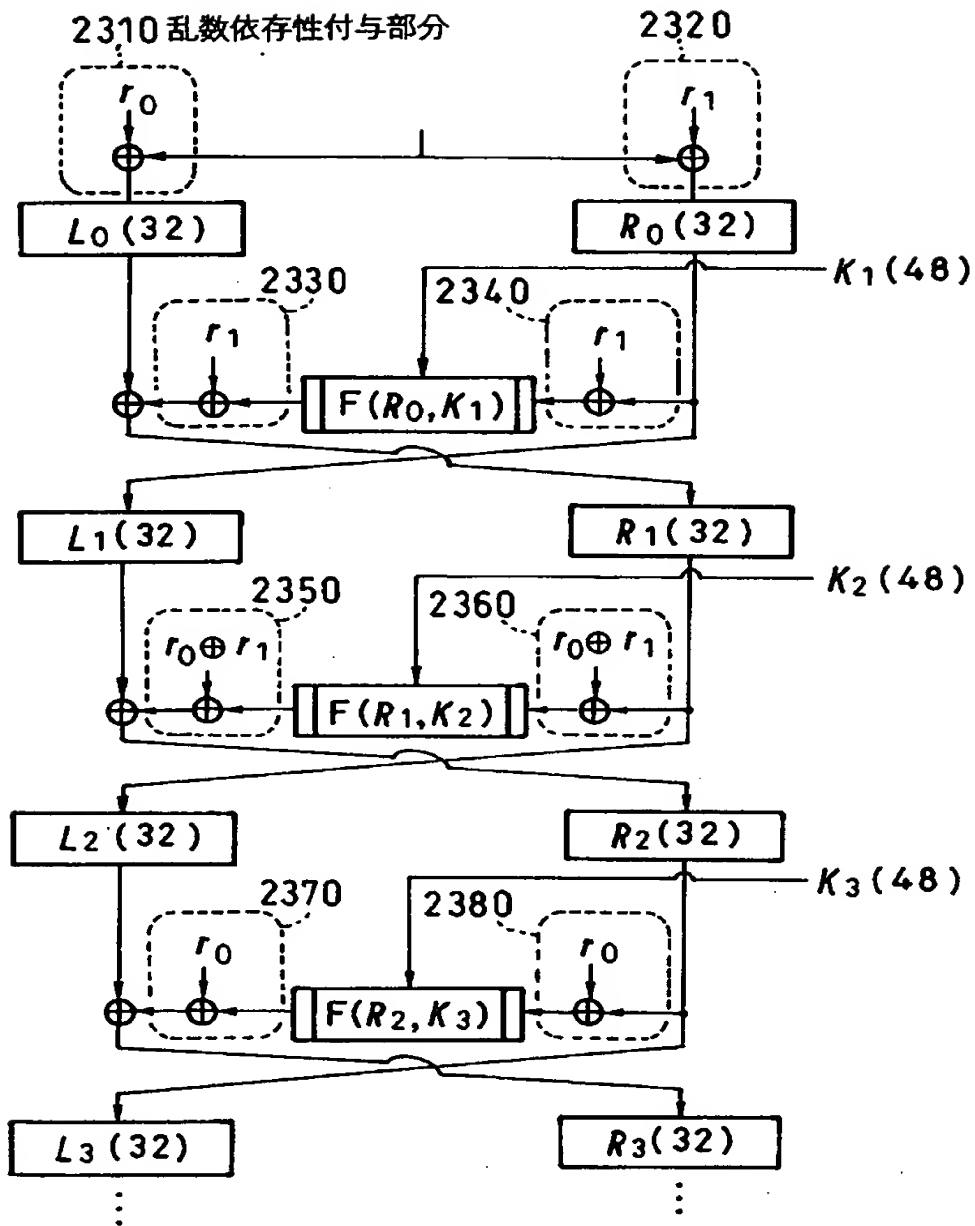
【図 2 1】



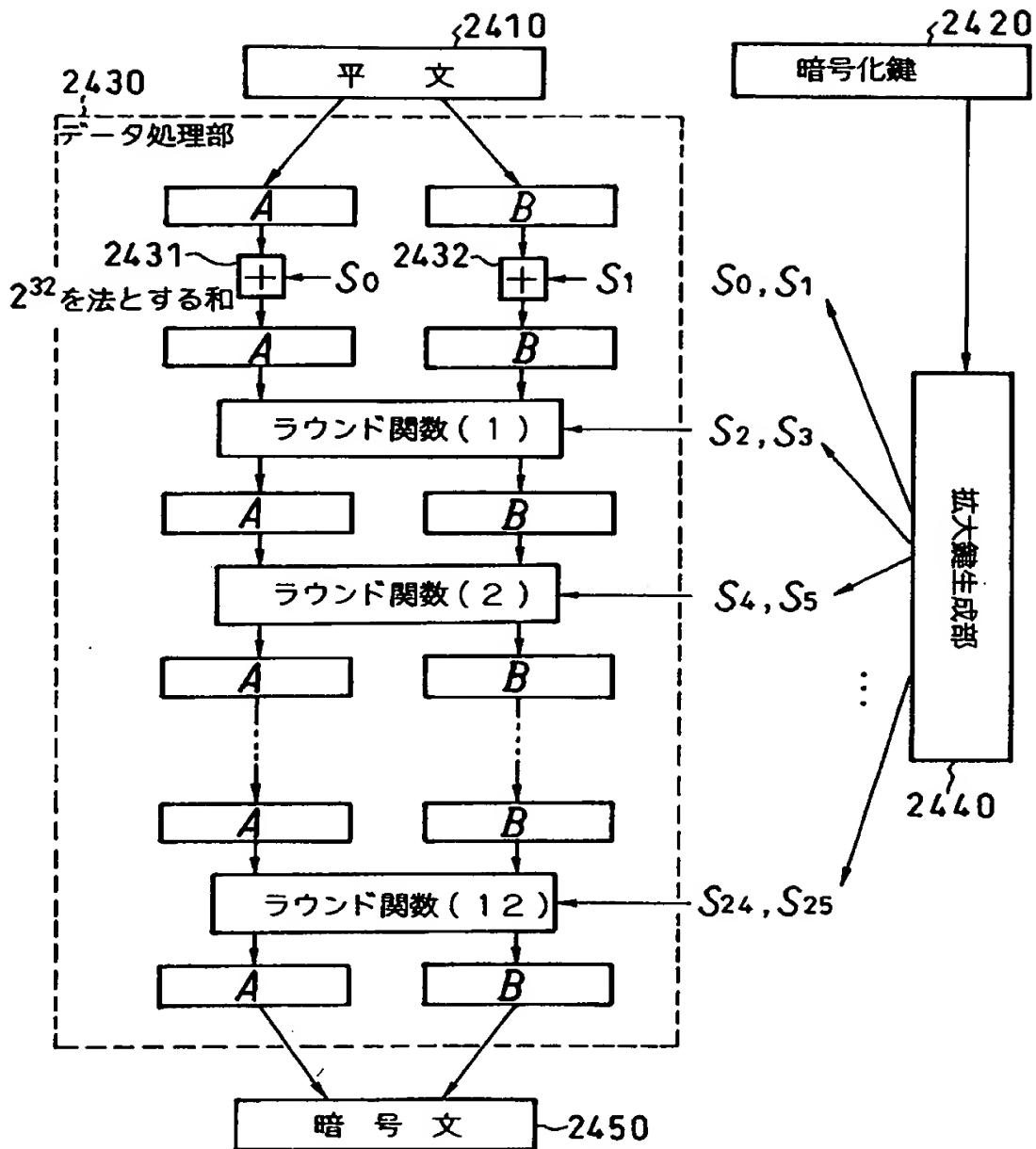
【図 2 2】



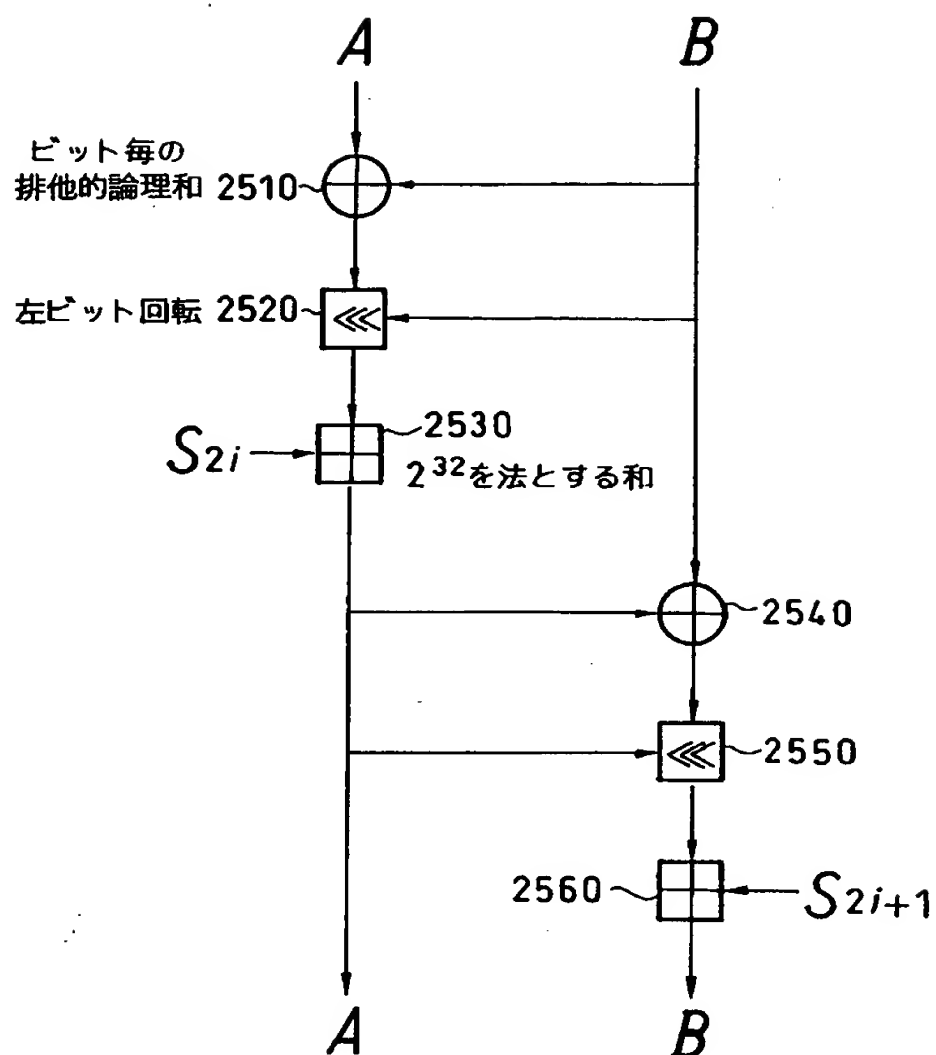
【图 2 3】



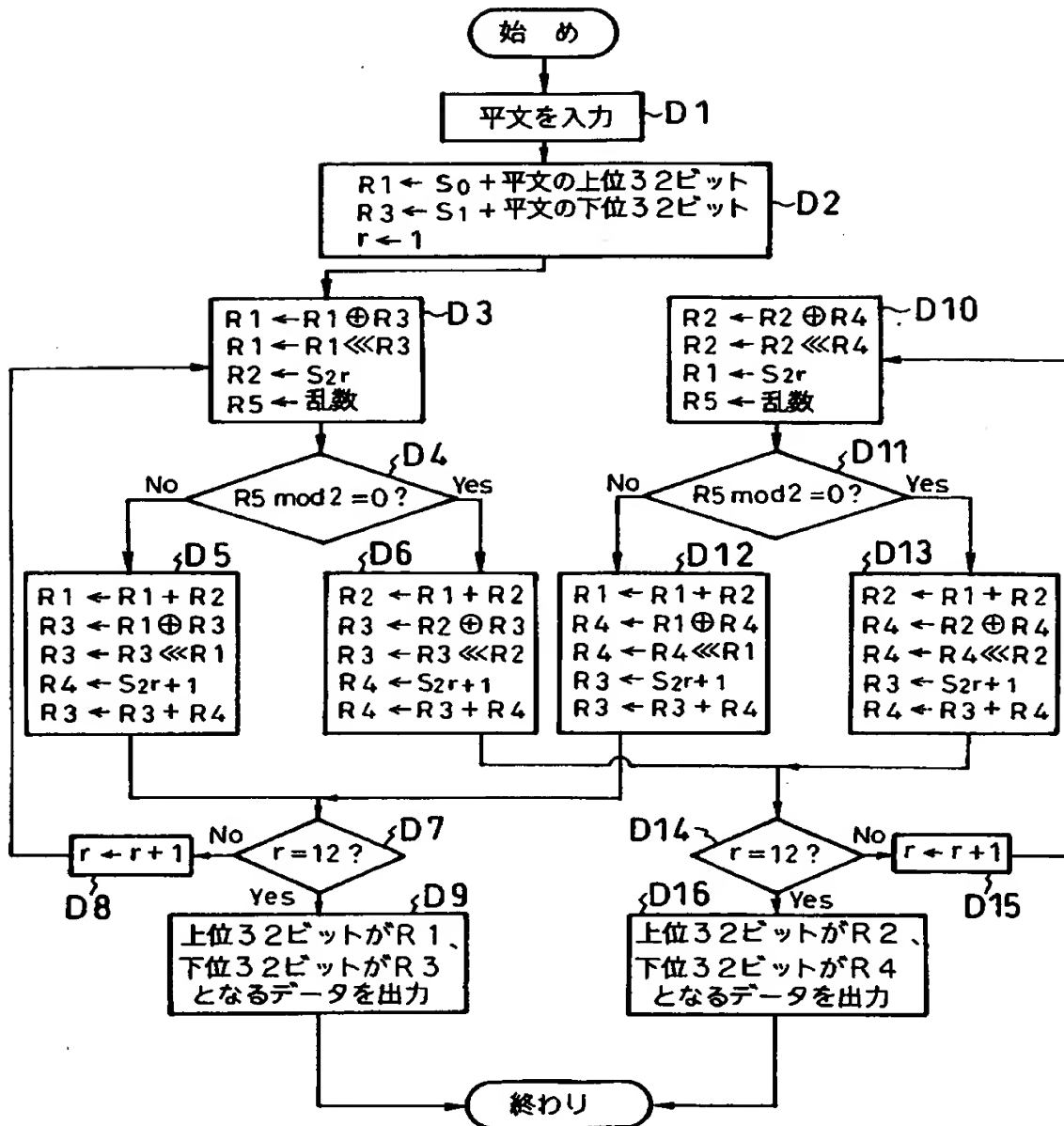
【図 2 4】



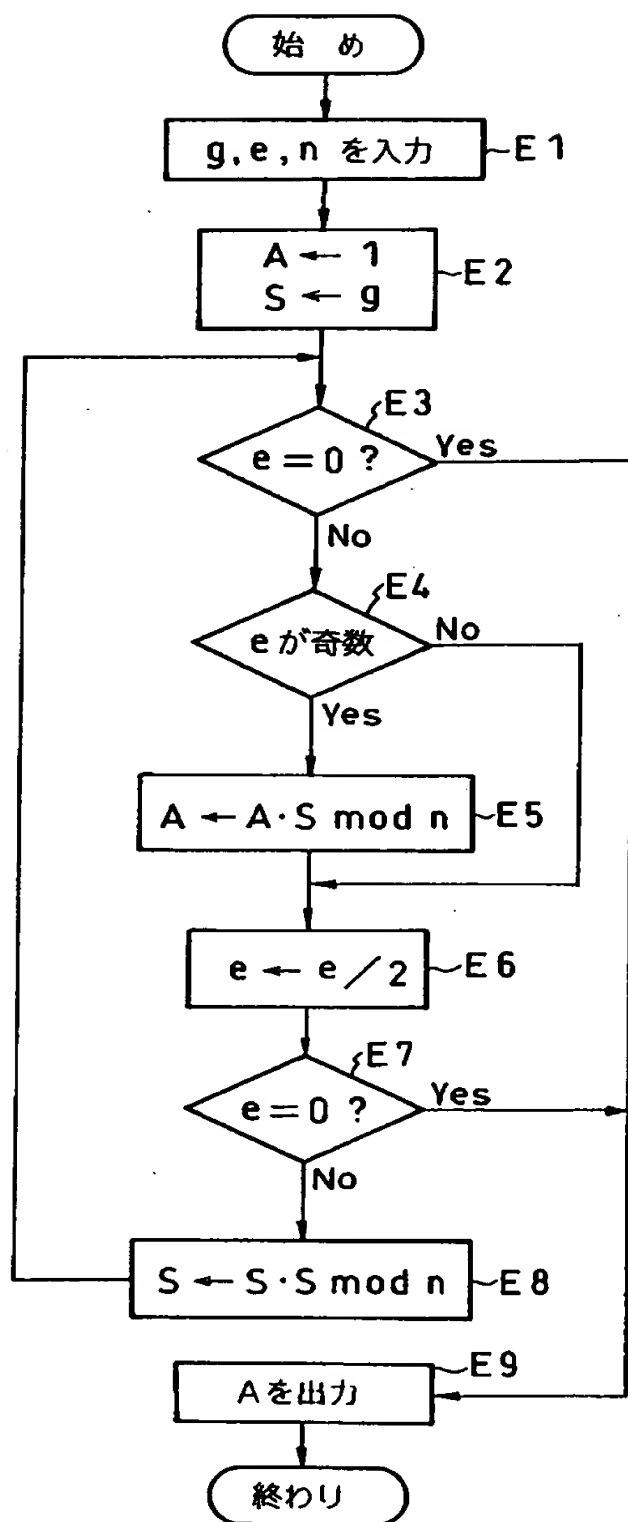
【図 2 5】



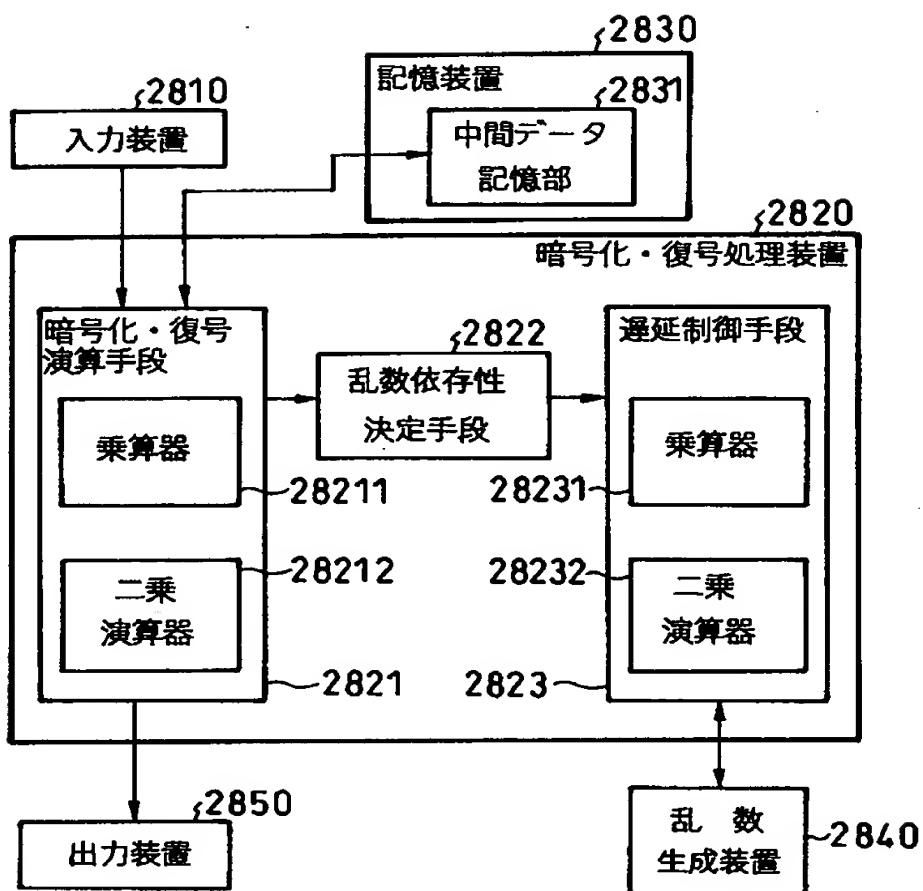
【図 2 6】



【図 2 7】



【図 2 8】



【書類名】 要約書

【要約】

【課題】 電力解析や電力差分解析等の消費電力の測定による暗号解析に対して耐性のある暗号化装置、復号装置、および暗号化・復号装置を提供する。

【解決手段】 中間データ制御手段 1 2 3 は、乱数生成装置 1 4 0 から出力される乱数を入力として、中間データを乱数に依存して変化させる乱数依存中間データ変更操作を中間データ変更要求の発生時点で行い、かつ当該乱数依存中間データ変更操作を複数回適用することによって乱数の効果を相殺するように制御する。暗号化演算手段 1 2 1 は、乱数依存中間データ変更操作に依存して状態を変化させつつ、平文に対する暗号化処理を実行し、乱数に依存しない暗号文を出力する。乱数依存性決定手段 1 2 2 は、暗号化処理の現在の処理段階が乱数依存中間データ変更操作を適用すべき処理段階であると判断した場合に、中間データ変更要求を発行する。

【選択図】 図 1

認定・付加情報

特許出願の番号	平成11年 特許願 第114230号
受付番号	59900384615
書類名	特許願
担当官	第七担当上席 0096
作成日	平成11年 4月23日

<認定情報・付加情報>

【提出日】	平成11年 4月21日
-------	-------------

特平 11-114230

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日 1990年 8月29日

[変更理由] 新規登録

住 所 東京都港区芝五丁目7番1号

氏 名 日本電気株式会社